U.S. Department of Transportation
United States Coast Guard

Commandant
United States Coast Guard

2100 Second Street, S.W.
Washington, DC 20593-0001
(202) 267-1302

COMDTINST M5500.13A
24 JUL 1987

COMMANDANT INSTRUCTION M5500.13A

Subj: Automated Information Systems (AIS) Security Manual

1. PURPOSE. This instruction provides U. S. Coast Guard policy, procedures, standards, and guidance for implementing the Automated Information Systems (AIS) security program.

2. DIRECTIVES AFFECTED. Commandant Instructions M5500.13 and C5500.14 are cancelled.

3. BACKGROUND. The Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, requires Federal agencies to assure an adequate level of security for all agency automated information systems, whether maintained in-house or commercially. Agencies must:

   a. assure automated systems operate effectively and accurately,

   b. assure appropriate physical, personnel, administrative, and technical controls are implemented, and

   c. assure the continuity of operation of automated systems that support critical agency functions.

   To achieve these objectives, agencies are required to implement and maintain an automated information systems security program which addresses four primary elements: applications security, personnel security, AIS facility security, and security awareness and training. The program must be consistent with government-wide policies, procedures, and standards issued by the Office of Management and Budget, the Department of Commerce, the Department of Defense, the General Services Administration, and the Office of Personnel Management. Programs must also incorporate additional requirements for securing national security information in accordance with appropriate national security directives.

4. DISCUSSION.

a. Automated information systems security addresses the protection of automated systems (hardware, software, and processing environment) and the protection of the information they contain. Government information is a valuable resource. As employees and agents of the government, we are accountable to the public at large for how we manage all government resources, including information. We have a continuing responsibility to protect the confidentiality and integrity of the information we use and to ensure essential agency functions are carried out.

b. AIS security is a management problem, not a technical one and the responsibility for protecting our information resources lies with each command and ultimately with each of us as individuals. Managers of automated systems must assess the risks of unauthorized modification and disclosure of information, and denial of service of their systems and then employ the controls needed to reduce those risks to an acceptable level. This instruction describes the requirements for an AIS security program which will allow commanding officers, AIS managers, and Coast Guard personnel who use automated systems to meet the requirements of OMB A-130 and their responsibilities to the public.

c. The Coast Guard AIS security program is new. AIS security policy and procedures will evolve as we learn more about how we can protect our automated systems and information. Constructive comments about the program and this Manual are welcome.

5. RESPONSIBILITIES.

a. Commandant (G-T) is the program director for the AIS security program; Commandant (G-TDS) is the program manager. Commandant (G-O) is the program director for Coast Guard security programs overall and Commandant (G-OIS) is the program manager. Commandant (G-TDS) shall ensure the AIS security program is consistent with overall Coast Guard security requirements as determined by Commandant (G-OIS).

b. Chiefs of Headquarters offices shall:

(1) Protect automated information systems and the information they contain by ensuring the AIS security program policies, procedures, and standards described in this instruction are followed.

(2) Designate an individual, called the ADP Security Officer (ADPSO), to implement the program and act as point of contact for AIS security matters. Notify Commandant (G-TDS) of the ADPSO's name, address, and phone number and update the information as changes occur.

5. c. Area and district commanders; commanding officers of Regional Maintenance and Logistics Commands; Commander, Activities Europe; and commanding officers of Headquarters units shall:

(1) Protect automated information systems and the information they contain by ensuring the AIS security program policies, procedures, and standards described in this instruction are followed.

(2) Designate an individual, called the ADP Security Officer (ADPSO), to implement the program and act as point of contact for AIS security matters. Notify Commandant (G-TDS) of the ADPSO's name, address, and phone number and update the information as changes occur.

d. All Coast Guard and contractor personnel shall use automated information systems only when authorized to do so. Each authorized user shall abide by the security requirements implemented for the system.

6. ACTION. Area and district commanders; commanders of maintenance and logistics commands; unit commanding officers; and Commander, CG Activities Europe shall ensure compliance with this Instruction.

7. REPORTS. The AIS Security Program Self-Audit Report, RCS-G-TDS-16232 is required per Chapter 15 of this manual.

/s/W. F. MERLIN
Chief, Office of Command, Control & Communications

(G-TIS-3)

2100 Second Street, S.W.
Washington, DC 20593-0001
(202) 267-1324

COMMANDANT INSTRUCTION 5500

Subj: CH-1 to COMDTINST M5500.13A, Automated Information Systems (AIS) Security Manual

1. PURPOSE. This notice provides change one to COMDTINST M5500.13A.

2. SUMMARY OF CHANGES. There is one significant change marked by a vertical line in the left margin.

   a. 6.E.: Guidance on application of ADP position sensitivity criteria is deleted. Commandant (G-OIS) shall be contacted when assistance is needed in determining ADP position sensitivity.

3. ACTION. Remove and insert the following pages:

| Remove | Insert |
|---|---|
| Pages i and ii | Pages i and ii, CH-1 |
| Pages 6-3 thru 6-5 | Pages 6-3 and 6-4, CH-1 |

/s/R. M. POLANT
Chief, Office of Command, Control & Communications

Encl: (1) CH-1 to COMDTINST M5500.13A

**TABLE OF CONTENTS**

**TABLE OF CONTENTS**

**TABLE OF CONTENTS**

**TABLE OF CONTENTS**

**ENCLOSURES**

ENCLOSURE (1) - AIS SECURITY DEFINITIONS

ENCLOSURE (2) - AIS SECURITY REFERENCES

ENCLOSURE (3) - MICROCOMPUTER RISK ASSESSMENT METHODOLOGY

ENCLOSURE (4) - STANDARD TERMINAL RISK ASSESSMENT METHODOLOGY **

ENCLOSURE (5) - GENERIC CONTINGENCY PLAN **

ENCLOSURE (6) - SENSITIVE APPLICATION DESIGN GUIDE (SADG) **

ENCLOSURE (7) - SENSITIVE APPLICATION CERTIFICATION (SAC) REVIEW METHODOLOGY **

ENCLOSURE (8) - SAMPLE AIS SECURITY PLAN **

ENCLOSURE (9) - OMB A-130, MANAGEMENT OF FEDERAL INFORMATION RESOURCES

Note: Double asterisks (**) denote those enclosures distributed separately, normally only to major commands and offices.

## CHAPTER 1. AIS SECURITY POLICY

**A. SCOPE AND APPLICABILITY.** Security requirements and guidance contained in this manual are applicable to all automated information systems owned by or operated on behalf of the Coast Guard. Systems which support Department of Defense or other department or agency missions are also subject to the security requirements of the supported department/agency.

**B. DEFINITIONS.**

1. Accreditation - The official authorization that is granted to an AIS facility to process classified or sensitive information in its operational environment. Accreditation is based on the determination the AIS is operating at an acceptable level of risk, after a comprehensive security evaluation and consideration of other management factors (e.g., criticality of operations, cost to implement controls, impact on operations, planned changes in AIS operations.)

2. AIS - See Automated Information System

3. AIS Activity - Any operating or staff unit of the Coast Guard operating an AIS, or commercial firm providing AIS services to the Coast Guard under contract.

4. AIS Security Staff - Individuals assigned responsibility for and who function as action officials for AIS security within their respective organization. An ADP Security Officer must be designated, as a minimum, at major commands (Headquarters' offices, area staffs, districts, and Headquarters' units, and Activities Europe); other staff designations provide for a hierarchy of responsibilities within the command and may be assigned at the discretion of the commanding officer. AIS security staff designations include:

   **ADP Security Officer (ADPSO)**
   **ADP Systems Security Officer (ADPSSO)**
   **Network Security Officer (NSO)**

5. Automated Information System (AIS) - Automated information systems include traditional ADP systems (mainframes and minicomputers), microcomputers, office information systems, networks which connect them, and applications (software) which run on them.

1.B.6. Certification - The official authorization that is granted to a sensitive application attesting to the adequacy of its security controls. Certification is made based on an independent review of security controls of the AIS facility and the application program and manual interfaces to determine if security design specifications are correct and have been properly implemented.

7. Contingency Plan - A contingency plan provides a course of action to be followed during or following an emergency or other abnormal event which causes or may cause a disruption in data processing services for essential functions (applications). Contingency plans address both the data processing support and the function itself.

8. Controls (or Countermeasures or Safeguards) - The physical, personnel, administrative, hardware, software, and communications measures used to protect against unauthorized (accidental or intentional) disclosure, modification, or destruction of automated systems and data, and denial of service to process data.

9. Data Sensitivity (LEVELs I, II, AND III) - Categories of data used to determine the degree of protection to be afforded data and automated information systems processing such data. This is a CG categorization which groups other recognized data/information categories for the convenience of prescribing automated information system security requirements.

   a. Level I. Classified data.

   b. Level II. Unclassified, sensitive data (called sensitive) requiring special protection; for example, Privacy Act, For Official Use Only, technical documents restricted to limited distribution.

   c. Level III. All other unclassified data.

10. Designated Approving Authority (DAA) - The DAA is the official having responsibility for the accreditation of an AIS.

11. Mode of Operation - The security environment and method of operating an AIS or network. Modes include: Multilevel Security, Controlled Security, Systems High Security, Dedicated Security Mode, Periods Processing, and Least Privilege.

B. 12. Office Information System (OIS) - Any electronic system designed and used solely for document management purposes; i.e., preparation (word processing), storage, retrieval, manipulation (sorting, indexing, etc.), and distribution (electronic mail). Office information system equipment excludes typewriters, office copy machines, and other devices which have no text editing capability.

13. Risk Assessment (or Risk Analysis) - An analysis of assets and vulnerabilities, and threats to those assets to determine the level of risk to an AIS. Risk is "measured" either quantitatively or qualitatively by determining the impact of threats on the facility, system, information, personnel, and supported organizations or other users.

14. Security - The effectiveness level of the controls which allow access to an AIS such that only properly authorized individuals, or processes operating on their behalf, will have access to read, write, create, or delete information, or interfere with the timely processing of information. Also the measures required to protect against unauthorized (accidental or intentional) disclosure, modification, or destruction of automated systems and data, and denial of service to process data. Components include Physical Security, Administrative Security, Personnel Security, and Technical Security (hardware, software, and communications).

15. Sensitive Application - The set of procedures (predominantly but not necessarily exclusively automated) which define the arithmetic computations and data handling operations of classified (Level I) or sensitive (Level II) data to achieve a specific purpose. An application has automated processes programmed in a language (e.g., assembly, BASIC, COBOL, Wang glossary) or off-the-shelf application package which permits automatic processing of the information. Text files or data base files containing (storing) but not processing sensitive information are not sensitive applications.

16. Sensitive Information (or Data) - Information that, as determined by a competent authority, must be protected because its unauthorized disclosure, alteration, loss, or destruction will at least cause perceivable damage to someone or something. Classified information is a separate category of information, and is always designated as classified (e.g., Confidential, Secret, Top Secret).

1.B.16. (Cont'd) The term sensitive information is sometimes used for unclassified, sensitive information. This type of information includes, but is not limited to, certain personal, budget, financial and management information, and information generally categorized as For Official Use Only (e.g., proprietary and privileged information).

17. Tempest - The study and control of spurious electronic signals emitted from electrical equipment.

18. Threat - The source of an adverse event that can cause a loss. Threats are categorized as either natural hazards, accidents, or intentional acts.

19. Trusted Computer System - A system that employs sufficient hardware and software integrity measures to allow its use for processing simultaneously a range of sensitive and/or classified information. The National Computer Security Center has defined application-independent evaluation criteria to classify systems into four broad hierarchical divisions of enhanced security protection with varying degrees of trust.

20. Vulnerability - A weakness in the physical layout, organization, procedures, personnel, management, administration, hardware, or software that may be exploited to cause harm to an automated information system.

**C. POLICY**. Coast Guard personnel shall:

1. Provide adequate and effective protection of all automated information system resources, including computer facilities and equipment, peripherals, remote terminals, programs, associated documentation, supplies, information, and personnel associated with computer operations.

2. Protect classified information and sensitive information handled by automated systems against espionage, sabotage, fraud, misappropriation, misuse, or inadvertent or deliberate compromise, specifically:

   a. Information classified, in accordance with Executive Order 12356, as important to national security,

   b. Unclassified, national security-related information which has been determined to have value to foreign adversaries as described in National Security Communications Advisory Memorandum (NACAM) 84/1,

1.C.2. c. Information regarding individual privacy of United States citizens as provided for in the Privacy Act of 1974 as described in COMDTINST M5260.2.

d. Privileged, proprietary, and other information properly designated "For Official Use Only," as described in COMDTINST M5500.11, Security Manual, and

e. Other information which must be protected from unauthorized disclosure, alteration, loss, or destruction because of possible damage to personnel or property.

3. Protect funds, supplies, and material managed or disbursed through the use of an automated information system from theft, fraud, misappropriation, or misuse. This includes automated asset/resource accounting or authorizing systems, operations which are involved in the control and distribution of funds, or the processing of information which offers the opportunity to divert economically valuable resources (e.g., supplies, dollars, or data).

**D. PROGRAM REQUIREMENTS.**

1. Each Headquarter's office, area staff, district, Headquarter's unit, and Activities Europe having an automated system shall have a qualified ADP Security Officer (ADPSO), appointed in writing, responsible for implementing the instructions contained in this Manual. In addition, ADP System Security Officers (ADPSSO), and Network Security Officers (NSO) shall be appointed as appropriate, in writing, to assist the ADPSO in implementing the AIS security program. See Chapter 2, Areas of Responsibility.

2. Classified and sensitive information handled by Coast Guard automated systems and associated telecommunications equipment and systems shall be properly safeguarded against unauthorized access, use, modification, destruction, or other denial of service through the integrated employment of appropriate physical, personnel, administrative, hardware, software, communications, and emanations security controls. See separate chapters for discussion of appropriate security controls.

3. Each automated information system shall be provided a level of security commensurate with the importance of system operation to overall mission accomplishment; the value, sensitivity, and criticality of the information being processed; the value of the facility, hardware, and software; and the relative risks to the system.

1.D.4. Each automated system shall be designated as classified, sensitive, or nonsensitive based on the sensitivity and criticality of information processed. The following criteria apply:

a. **Classified (Level I)** - Classified information including Confidential, Secret, Top Secret, and higher.

b. **Sensitive (Level II)** - Information requiring protection under the provisions of the Privacy Act of 1974, unclassified national security-related information, information designated "For Official Use Only," and other information which relates to asset/resource, proprietary, or contractual information.

c. **Nonsensitive (Level III)** - Information which does not warrant a higher designation.

5. Each activity having an automated system shall develop, maintain, and periodically test contingency plans which address emergency response, back-up, and recovery actions required to provide reasonable continuity of data processing support should events occur that prevent normal operations. See Chapter 4, Contingency Planning.

6. Each Headquarter's office, area staff, district, Headquarter's unit, and Activities Europe having an automated system handling classified or sensitive information shall establish a formal risk management program to assist in identifying and assessing relative threats, vulnerabilities, and risks, as well as controls to reduce risks to an acceptable level. See Chapter 3, Risk Management and Risk Assessment.

7. Each activity having an automated system designated classified or sensitive shall undergo a periodic and detailed review leading to formal accreditation, the formal approval of a system to be operated at what has been determined to be an acceptable level of risk. See Chapter 13, Accreditation.

8. For each activity having an automated system with a classified or sensitive designation, positions whose purpose and function merit such, shall be designated ADP sensitive. See Chapter 6, Personnel Security.

1.D.9. Military and civilian personnel who will be involved in classified or sensitive computer operations and who will occupy positions designated ADP sensitive, shall be appropriately cleared and granted access prior to occupying such a position. Interim clearance and access may be authorized, where deemed necessary, by the activity commanding officer.

10. For each newly acquired automated information system:

    a. All requirements (e.g., general functional systems requirement, detailed functional systems requirement, or statement of work) for systems handling, or intended to handle, sensitive or classified information shall contain provisions for appropriate security controls.

    b. Appropriate security-related specifications shall be included in all hardware and software procurement or acquisition packages.

    c. In no event will hardware, software, or services be procured for use in systems handling classified or sensitive information without full prior consideration of the requirements of this Manual.

    See Chapter 19, New Systems - Security Requirements.

11. When two or more data processing installations connect to a network within a single command, a Network Security Officer (NSO) shall be designated to establish appropriate security requirements for network users. Users of the network shall fully implement security controls prescribed by the NSO.

12. When one or more data processing installations connect to a network involving two or more commands (e.g., a Coast Guard-wide or inter-district network), each command shall designate a Network Security Officer (NSO). The NSO shall establish, in conjunction with the network manager, appropriate security requirements for network users within the command for which the NSO is responsible. Users of the network shall fully implement security controls prescribed by the NSO.

1.D.13. For those systems relying upon remote terminal devices:

a. Security characteristics of remote terminals and interface devices, if required, as well as security measures for the areas in which they are located, shall be prescribed by the organization having security responsibilities for the central computer.

b. Measures and procedures required to ensure overall system integrity shall be agreed upon before remote terminals and other supporting devices are connected to the central computer.

b. Remote terminal user organizations shall comply with approved security measures and compliance with security procedures issued by the host central computer installation.

14. Each Headquarter's office, area staff, district, Headquarter's unit, and Activities Europe shall establish a security awareness and training program to assure Coast Guard and contractor personnel involved in the management, operation, programming, maintenance, or use of automated systems are aware of their security responsibilities and know how to fulfill them.

15. Each Headquarter's office, area staff, district, Headquarter's unit, and Activities Europe shall report the results of an AIS Security program self-audit to Commandant (G-T) annually. See Chapter 15, AIS Security Documentation Requirements.

**E. WAIVERS**. When a commanding officer believes the requirements of this manual cannot be met without adverse impact on operations; he may submit a request for waiver of specific requirements to Commandant (G-TDS) via the chain of command. The request for waiver must provide information in sufficient detail to clearly demonstrate the relationship between the requirement and the adverse impact. Inquiries for guidance and interpretation are encouraged and should be addressed to Commandant (G-TDS).

**F. CONFLICTS**. The AIS Security Program is a sub-program within the broader Coast Guard Security Program. In the event of conflict between the requirements of this manual and COMDTINST M5500.11, Security Manual, the requirements of COMDTINST M5500.11 shall take precedent. Conflicts in requirements may also occur when other department/agency security requirements are applicable. When a commanding officer determines that a conflict in requirements exists, he shall notify Commandant (G-OIS) and (G-TDS) of the conflict in writing.

## CHAPTER 2. AREAS OF RESPONSIBILITY

**A. PROGRAM MANAGEMENT.** The Chief, Office of Command, Control, and Communications (G-T) is the program director for the AIS security program; the Chief, Data Systems Division (G-TDS) is the program manager. The Chief, Office of Operations (G-O) is the program director for Coast Guard security programs overall and Chief, Intelligence, Investigations and Security Division (G-OIS) is the program manager. Commandant (G-TDS) will ensure the AIS security program is consistent with overall Coast Guard security requirements as determined by Commandant (G-OIS).

1. Commandant (G-TDS):

   a. Establishes AIS security policies, standards, and procedures.

   b. Prepares, updates, and disseminates the AIS Security Manual.

   c. Coordinates the Coast Guard-wide implementation of the AIS Security program.

   d. Provides generic or model AIS Security Plan, contingency plans (for disaster recovery and continuity of operations), and other AIS security documentation.

   e. Approves Coast Guard risk assessment methodologies.

   f. Coordinates or assists in the performance of risk assessments of automated information systems.

   g. Coordinates or assists in the certification of sensitive applications.

   h. Assists in the security test and evaluation of automated information systems when required.

   i. Provides technical recommendations to those responsible for AIS accreditation and sensitive application certification.

   j. Coordinates an AIS security training and awareness program.

   k. Is custodian of AIS security documentation.

2.A.2. Commandant (G-TTS):

a. Establishes communications security (COMSEC) security policies, standards, and procedures.

b. Establishes TEMPEST security policies, standards, and procedures.

c. Assists Commandant (G-TDS) in the performance of risk assessments when requested.

3. Commandant (G-OIS):

a. Performs oversight inspections and reviews of Coast Guard security programs.

b. Establishes policy, standards, and procedures applicable to the physical protection of installations housing automated systems.

c. Participates in the performance of risk assessments and security test and evaluations when requested.

d. Establishes policy, standards, and procedures concerning civilian employee security clearances.

e. Determines the position sensitivity and the investigative requirements for civilian AIS positions.

f. Investigates security violations resulting from theft, fraud, or misuse of equipment.

**B.** PROGRAM IMPLEMENTATION.

1. Chiefs of Headquarter's offices, area and district commanders; commanding officers of Regional Maintenance and Logistics Commands; Commander, Activities Europe; and commanding officers of Headquarters units implement AIS security policy, standards, and procedures contained in this Manual within their command or office, including:

a. Designate and appoint in writing an ADP Security Officer (ADPSO) to act as the focal point for all command or office AIS security matters. Notify Commandant (G-TDS) of the ADPSO's name, address, and phone number and update the information as changes occur.

b. Ensure a single management official (ADPSSO or NSO) is assigned responsibility for the security of each automated information system or network within the command or office.

2.B.1. c. Ensure contingency plans are prepared for each automated system and critical function (application).

d. Ensure a risk assessment is conducted for each automated system and network.

e. Grant or request systems accreditation in accordance with guidance in Chapter 13, Accreditation.

f. Ensure each office, area, district, or Headquarter's unit-unique sensitive application is certified based on formal review of application security controls.

g. Ensure appropriate personnel security procedures are established and enforced for those personnel operating or using automated systems.

h. Ensure AIS security awareness and training is provided Coast Guard and contractor personnel operating and using automated systems.

i. Ensure contract specifications for AIS hardware, software, services, and supplies contain appropriate security requirements.

Detailed responsibilities for AIS security staff and command security manager are defined below.

2. AIS Security Staff. The AIS security staff organization will vary within each Headquarters office, area, district, Headquarter's unit and Activities Europe. AIS security staff positions and responsibilities are:

- ADP Security Office (ADPSO) - Headquarters office, area, maintenance and logistic command, district, and Headquarter's unit level.

- ADP Systems Security Officer (ADPSSO) - Any activity (e.g., division, branch, district unit) having an automated information system.

- Network Security Officer (NSO) - Headquarters office, area, maintenance and logistic command, district, and Headquarter's unit level.

Large commands might have a different individual assigned to each position while in smaller commands one individual might assume the duties for all positions. The commanding officer ultimately has the discretion as to the resources applied within his command to meet the requirements contained in this Manual.

2.B.2. a. ADP Security Officers (ADPSO) coordinate Headquarters office, area, district, or Headquarter's unit implementation of the AIS security program, including:

(1) Be the focal point for all AIS security matters for the the command.

(2) Ensure an ADPSSO and NSO are assigned in writing where applicable.

(3) Develop and maintain an AIS Security Plan to protect command or office automated information systems. Submit a copy of the AIS Security Plan to Commandant (G-TDS).

(4) Maintain an inventory of automated systems, sensitive applications, and essential functions (applications) supported by an automated system.

(5) Coordinate or assist in the preparation and maintenance of contingency plans for automated systems and essential applications.

(6) Coordinate the implementation of the command or office risk management program and assist in the performance of risk assessments, sensitive application certification reviews, and security test and evaluations.

(7) Ensure command or office accreditation support documentation is developed and maintained and accreditations and requests for accreditation of automated systems and networks are completed as required.

(8) Coordinate with the command security manager for OIS program on matters concerning AIS security issues in accordance with the security organization structure established by the commanding officer.

(9) Promptly report all AIS security violations to the commanding officer. Copies of reports shall be forwarded to Commandant (G-OIS) and (G-TDS) via the chain of command.

(10) Be custodian of command or office AIS security documentation.

2.B.2. a. (11) Assume the AIS security staff responsibilities for any staff member not appointed.

(12) Conduct an annual AIS security program self-audit and provide self-audit review results for all activities within the command or office to Commandant (G-TDS).

b. ADP System Security Officers (ADPSSO) assist the ADPSO in implementing the AIS security program, including:

(1) Be the focal point for all security matters for automated systems for which assigned.

(2) Implement the AIS security program as it applies to assigned automated systems.

(3) Maintain an inventory of automated systems, sensitive applications, and essential functions (applications) supported by an automated system and security survey for each system.

(4) Provide input to the ADPSO for the AIS Security Plan with regard to all assigned automated system(s).

(5) Prepare and maintain contingency plans for assigned system and critical applications.

(6) Conduct or assist the ADPSO in the performance of risk assessments, sensitive application certification reviews, security test and evaluations, and audits for assigned system.

(7) Implement appropriate security controls required by directive or determined to be cost-effective by the activity.

(8) Monitor system activity, including identification of the levels and types of data handled by automated systems, assignment of passwords and review of audit trails, outputs, etc., to ensure compliance with security directives and procedures.

(9) Maintain liaison with remote facilities served by automated systems to ensure compliance with applicable security requirements.

2.B.2. b. (10) Provide annual self-audit review results to the ADPSO.

c. Network Security Officers (NSO) assist the ADPSO in implementing the AIS security program, including:

(1) Ensure controls and requirements are included in the network design and that individual nodes of the network comply with these controls and requirement, prior to connecting to the network. Security requirements will be agreed to in writing by the network DAA and the DAA of the network node (i.e., automated information system connected to the network.

(2) Develop and promulgate the standard security procedures governing network operations.

(3) Ensure all required network controls are utilized and controls used at network nodes fully support the security integrity of the network.

(4) Maintain liaison with all ADPSSO in the network.

d. Command Security Managers:

(1) Ensure adequate physical protection of the installation housing the AIS facility is provided.

(2) Assist in the performance of risk assessments.

(3) Assist in the performance of security test and evaluation.

(4) Assist ADPSO in managing an AIS security awareness and training program.

3. Commanding officers or managers of AIS activities within offices, areas, districts, regional maintenance and logistics commands, or Headquarter's units must implement those security controls necessary to protect the automated information systems and information within their command or organization. The requirements and guidance provided by this Manual, the ADPSO, ADPSSO, and NSO, are used where applicable.

2.B.4. Headquarter's program managers who sponsor (i.e., design, develop, acquire, or implement) automated information system hardware, software, network, or sensitive application projects must ensure the system they sponsor provides adequate security as determined by the requirements of this Manual. Where an automated system is or will be run at multiple activites or sites, the sponsoring program manager is responsible for ensuring the system has been certified in accordance with this Manual for multi-site distribution.

5. Contracting officers who administer contracts for AIS hardware, software, maintenance, supplies, or services ensure that contract specifications comply with the security requirements of this instruction.

a. Solicitation specifications will include, where applicable, the following:

(1) Rules of conduct which a contractor and contractor employees must follow.

(2) A description of the personnel security clearances required for access.

(3) A description of the controls the contractor and the systems must provide.

(4) A list of the Department of Transportation and Coast Guard directives or other policies, standards, and procedures that apply.

(5) Methods and procedures which will be used to determine the effectiveness of the controls.

(6) A requirement that the risks be periodically re-evaluated and that the activity's contracting organization be advised when new countermeasures are required.

b. When a contractor is being considered, the activity's contracting officer, with assistance from the AIS security staff, will evaluate the proposal or offer for award considering AIS security requirements including:

(1) A determination that the proposal demonstrates that the contractor will provide adequate protection;

2.B.5. b. (2) A legally enforceable provision that all controls applicable to the contractor will be in effect before commencing contract performance;

(3) A declaration as to whether the contractor or the government owns and/or manages the controls designed or developed for this contract.

6. Each user authorized to use an automated information system abides by the security requirements implemented by the AIS security staff (ADPSO, ADPSSO, and NSO) as applicable and only for authorized purposes. The user informs the AIS security staff of the levels and types of data they process or access.

7. All Coast Guard and contractor personnel shall use automated information systems only when authorized to do so.

## CHAPTER 3. RISK MANAGEMENT AND RISK ASSESSMENT

### A. RISK MANAGEMENT PRINCIPLES.

1. Security is a management problem. Risk management is an element of management science concerned with identifying, measuring, and minimizing the effects of unknown future events and their potential adverse consequences. A good risk management program can assist a manager in optimizing the amount of security for his automated information system (AIS).

2. A risk management program requires a critical examination - a risk assessment - of the AIS environment and the risks to which AIS assets are exposed. A risk assessment consists of an analysis of threats and vulnerabilities to the AIS and provides a basis for determining how much protection currently exists and how much additional protection is required. Risk assessment methodologies vary depending on the characteristics of the AIS; the methodology for evaluating risks for microcomputers differs from that of a mainframe computer. Although some minimum requirements for security controls exist, each AIS site must be evaluated separately to determine the appropriate controls for that site since each site and operating environment is different. Security controls are implemented after consideration of: the AIS exposure to risk (from the risk assessment), value of assets, critically of operations, cost (funds and personnel) to implement controls, impact on operations, planned changes in AIS operations, and other factors important to management. Risk management is an ongoing effort; risks must be reevaluated periodically and whenever changes occur to the AIS environment to ensure adequate protection is achieved.

3. The objective of risk management is to achieve cost-effective controls (safeguards) against deliberate or inadvertent:

   a. Loss/destruction of assets. Assets include system hardware, system software, application software, documentation, and data.

   b. Modification of assets. Assets include system hardware, system software, application software, documentation, and data.

   c. Unauthorized disclosure of information. Information includes classified, privacy, financial, asset, proprietary or any other type deemed worthy of protection.

3.A.3. d. Denial of service. This includes intentional or accidental loss in system reliability or continuity of operations.

4. The risk management program considers risks in the following automated information system environments: physical, administrative, personnel, hardware, software, communications, emanations, and data (information).

**B.** RISK ASSESSMENT PRINCIPLES. A risk assessment is an analysis of assets and vulnerabilities, and threats to those assets to determine the level of risk to an AIS. Risk is "measured" either quantitatively or qualitatively by determining the impact of threats on the facility, system, information, personnel, and the supported organizations or other users. While the complexity of the risk assessment depends on the scope and characteristics of the AIS under review, the following elements are always considered in the analysis.

1. Varying Security Requirements. Not all applications, systems, or facilities require the same level of protection. To determine the relative importance of each application and the facility itself, a systematic assessment must be used to determine the effect of unauthorized data disclosure, manipulation, destruction, and the effect of loss of data processing capabilities for varying periods of time.

2. Threats. A threat is any action or event, whose occurrence is likely to adversely affect the facility or system; the potential for harm from a particular source. Major threat groupings are: natural hazards, accidents, and intentional acts.

(a) Natural disaster - tornado, hurricane, earthquake, flood, lightning, windstorm, fire, rain, mud, ice, snow, etc.

(b) Accidents - unintentional acts caused by computer programmers, computer operators, maintenance personnel, or data processing customers.

(c) Intentional acts - deliberate acts causing damage or disruption by anyone including an unauthorized user of the system, or an authorized, disgruntled user.

3. Vulnerabilities. A vulnerability is a weakness that may be exploited by a threat agent to cause harm to the AIS activity. General factors considered in determining vulnerability include the geographical location, the operational and security modes, the sensitivity and

3.B.3. (cont'd) volume of data being handled, and the overall critically of the AIS operation. The more complex the operation, the more susceptible the site. The latter may be composed of large scale, multi-user, on-line, shared operations which may be made more vulnerable depending upon the privileges extended to the users. Simple query privilege represents a lesser vulnerability than that found in systems where the user has programming capability. Existing security controls must be taken into account when determining vulnerabilities. The existing level of security must be evaluated and any weaknesses in the current system of physical, administrative, and technical controls identified and documented. The existence of vulnerabilities has a direct relationship to the threat occurrence ratio.

**C. RISK MANAGEMENT PROGRAM.**

1. General. The Coast Guard risk management program involves an iterative process composed of the following elements:

   a. Activity AIS Security Plan.

   b. Risk Assessment.

   c. Security Controls Selection, Implementation, and Effectiveness Review.

   At the completion of these steps, a basis exists for determining what risks are present in the AIS environment, documenting the AIS security posture, and deciding whether or not to expend funds to enhance AIS security. A description of the three phases of the Coast Guard risk management process is given below:

2. Activity AIS Security Plan. The Activity AIS Security Plan summarizes activity AIS security policy and provide guidelines for all AIS security procedures to be used by the activity. The plan is the most important activity level document for implementing the security policies set forth in this instruction. The security plan establishes local security policies; defines security program scope and objectives; and assigns responsibilities to carry out the provisions of this instruction at the local level. It should address both short range and long range security goals of the activity. It addresses all aspects of AIS security (i.e., physical, personnel, administrative, hardware, software, communications, emanations, and data for the AIS activity). The plan should be a living document for the management and control of the total AIS security environment of the

3.C.2. (cont'd) activity. The plan will achieve maturity after three phases: (a) initial development, (b) update after the initial risk assessment, and (c) update after selection, implementation and test of security controls. Thereafter the plan will be updated after any significant changes to the system or subsequent risk assessments.

3. Risk Assessment. Risk assessments are divided into two basic categories as follows:

a. Quantitative. This type of risk assessment methodology is aimed at the mainframe and minicomputer environments. It provides management with an understanding of the potential risk as measured by the expected annual loss exposure in resources (dollars, productivity, etc.) and identifies how the loss will affect users of the system. It results in the quantitative evaluation of the degrees of damage or loss associated with each threat. For example: What is the probability of loss of a tape library and what are the economic and operational consequences of that loss? This evaluation forms the basis for action to manage the risk by identifying effective security controls and the cost of implementing those controls. The quantitative risk assessment process consists of the following steps:

- Planning and Organizing.

- Value Analysis.

- Threat and Vulnerability Analysis.

- Loss Exposure Analysis.

- Control Selection and Cost.

- Cost-Effectiveness Analysis.

Plan and Organize. Depending on the facility being reviewed and the availability of resources, the risk assessment may be accomplished by CG personnel or by contract. The risk assessment team is selected and a Risk Assessment Plan prepared. The level of effort and schedule for completing the risk assessment is established and responsibilities assigned.

Value Analysis. The cost and time to repair or replace AIS hardware, software, and facilities and correct or recreate information is estimated. The cost of disclosure of information is also estimated.

3.C.3. a. Threat and Vulnerability Analysis. Individual threats relevant to the facility undergoing risk assessment are identified. Threat identification is a difficult analytical process which must consider both known and reliably postulated threats. Threats may be actual, in which case there is documented evidence of a harmful event having occurred previously, or they may be postulated. Lack of evidence of threat agent activity can be expected since penetration of systems is difficult to detect by current audit procedures. Threat occurrence rates are derived by analyzing identified weaknesses and establishing a likelihood of occurrence. A vulnerability analysis evaluates existing physical, technical, and administrative controls. Vulnerabilities are usually controllable; the remainder of the risk management process seeks to develop cost-effective techniques for reducing the level of risk.

Loss Exposure Analysis. The results of the previous two steps are combined to compute a quantified measure of risk exposure. This quantified measure is the Annual Loss Exposure (ALE). The ALE is used to reduce the wide range of threats and vulnerabilities to a common denominator, the expected loss in dollars per year. ALE is the estimated dollar loss per event multiplied by frequency of occurrence of that event per year. When the ALE is known for each identified threat, threats may be rank-ordered to identify unacceptable risk exposures and to prioritize the selection of security controls. Additionally, the sum of all ALE's represents the total risk exposure for the ADP system/facility on an annualized basis.

Security Control Selection and Cost. Security controls identification is the process of reviewing identified risks (loss potential) and determining appropriate remedial action. Alternate ways of avoiding, preventing, detecting, minimizing, and recovering from the occurrence of threats are proposed and their cost estimated. Effective controls should be derived from cost/benefit or other types of economic and value assessment. Identification of areas of exceptionally high or unacceptable risk must be directly related to organizational mission, goals, and objectives as stated by the commanding officer.

3.C.3. a. Cost-Benefit Analysis. In this phase, the judgment of the risk assessment team as to the acceptability of various controls is reviewed by an appropriate management official. When this review has been completed, management approves controls which effectively reduce the degree of risk to an acceptable level. Security controls may have significant operational, budgetary, and time implications. Management will have the information needed to decide between risks and cost considerations.

b. Qualitative. This type of risk assessment methodology is targeted towards the microcomputer environment. The qualitative risk assessment acheives it's intended results in a more intuitive format by means of a checklist or survey format. A user completes a questionnaire and based on the responses, calculates or tallies the results which may be compared against predetermined baseline values to establish the current security posture of the installation. The baseline values or controls are a function of the required security for the type of processing being performed. Checklists and baseline controls must be used with caution since they don't necessarily ensure adequate protection at a given site; each computer site and operating environment is different.

4. Security Control Selection, Implementation and Effectiveness Review.

a. Security control selection. A well conducted risk assessment will normally result in the identification of numerous interrelated controls. In this phase, the risk assessment team evaluates the acceptability/unacceptability of various controls based on their cost and effectiveness and selects those which will reduce the degree of risk to an acceptable level. The commanding officer must approve security controls based on cost (funds and personnel) to implement them, impact on operations, planned changes in AIS operations, and other factors important to management.

To properly select security controls, the commanding officer must consider the possible degradation of operations by the controls. There may be significant disruption of managerial, operational, and administrative procedures attributable to these controls. Because of the potential effect on the organization, only the commanding officer can

3.C.4. a. (cont'd) properly make the choice between security and operational requirements. This requires understanding by the commanding officer of the degree of organizational dependence upon AIS and its importance to mission accomplishment.

There may be instances where the criticality of a function is such that the risks imposed by the use of AIS are unacceptable or that the controls required to achieve an acceptable level of security are impractical or impossible to implement. In these cases, the commanding officer may determine that automated support is unwarranted and unnecessary to manage adequately the risk to mission accomplishment. Except for controls mandated for classified information processing, the commanding officer is the final authority in any conflict between operational and AIS security considerations.

b. Security control implementation. The commanding officer is responsible for preparing a plan to implement controls which provide a cost-effective level of security. In preparing the plan, the commanding officer must consider the risk potential resulting from growing dependence upon automated systems; the magnitude of the security problem; and the potential effect on organizational resources.

c. Security control effectiveness review. Organizational and operational changes as well as changes in threats, demand continuing review of the effectiveness of security controls to achieve the optimum level of AIS security. Effectiveness review is an important process in documenting security techniques and ensuring that an applied technique has not created a more serious vulnerability of risk. The collective effectiveness of applied security controls provide the basis for future security actions and assist in identifying problem areas and additional security requirements.

Activities needing assistance in developing or implementing their risk management program should contact Commandant (G-TDS) for assistance.

**D. RISK ASSESSMENT REQUIREMENTS.** AIS security risk assessments shall be accomplished as follows:

1. Prior to the approval of design specifications for all new Coast Guard computer installations and facilities.

3.D.2. Whenever there is a significant change to the physical facility, hardware configuration, system software configuration, or application system.

3. At least every five (5) years for existing installations and facilities.
[Reference: OMB A-130, Management of Federal Information Resources dated 12 December 1985]

**E. PERFORMANCE OF RISK ASSESSMENTS.**

1. Mainframes and minicomputers.

a. The International Security Technology/Risk Analysis and Management Program (IST/RAMP) shall be used for mainframe and minicomputer systems. Initial risk assessments will be funded by Commandant (G-TDS). Subsequent analyses shall be performed by local personnel with technical assistance by Commandant (G-TDS). Risk assessments of computer facilities may be accomplished by either Coast Guard personnel or contractors. If contractors are to be used, approval must be granted by Commandant (G-TDS).

b. IST/RAMP is an automated quantitative model of an AIS security environment which runs on Transportation Computer Center's Amdahl. RAMP is used to assist analysts in estimating future losses to automated systems caused by damage, delay, fraud, disclosure, and theft threats. RAMP can also be used to evaluate alternative off-site back-up strategies for master files. RAMP users require an Amdahl user ID and data library, which may be obtained from Commandant (G-TDS). Since RAMP provides numerous analytical capabilities, training is usually required; Commandant (G-TDS) can provide additional information.

2. Standard Terminals. The Standard Terminal Risk Assessment Methodology (STRAM) provided as a separate enclosure to this Manual shall be used for all standard terminal systems.

3. Other Microcomputers. The "Other Microcomputer" risk assessment methodology provided as a separate enclosure to this Manual shall be used for other microcomputers and office information systems.

## CHAPTER 4. CONTINGENCY PLANNING

**A. GENERAL.** A contingency plan provides a course of action to be followed during or following an emergency or other abnormal event which causes or may cause a disruption in data processing services for essential functions (applications). Contingency plans address both the data processing support and the function itself. In most cases separate plans should be prepared for the AIS facility providing data processing support and for the individual functions. Contingency plans for AIS facilities (also called disaster recovery and continuity of operations plans) provide for reasonable continuity of data processing support. Contingency plans for applications provide for continuity of essential functions by program managers and end users in the event automated support is interrupted. The application contingency plan should be consistent with the contingency plan for the AIS activity at which the application is processed. Plans for systems which support essential functions of the activity should be fully documented and operationally tested periodically.

**B. POLICY.** Program managers and end users of AIS applications are responsible for establishing and maintaining alternative arrangements by which they can continue to deliver those products and services deemed essential in the event of a disruption of the primary source(s) of data processing support, where applicable.

Managers of AIS facilities are responsible for maintaining plans for continuing to provide operational support for essential functions, considering the needs of their users to the maximum practicable extent. Program managers, end users and AIS facility managers must coordinate their plans closely with each other to achieve essential and cost-effective support. Where essential functions are involved, plans are to be thoroughly documented, periodically tested, and updated as necessary to reflect changes in circumstances.

**C. REQUIREMENTS.**

1. Each application owner and end user accountable for an essential function using data processing support shall:

   a. Determine and document the essentiality of the products and services of the pertinent automated information systems.

   b. Notify the cognizant AIS facility manager of the essentiality of each automated information system supporting the function, and subsequently withdraw these notifications when applicable.

4.C.1. c. Develop, document, test, and keep current a contingency plan for delivering the products and services of each essential function in the event of a disruption of the primary source of AIS support. To the degree practicable, these plans should be consistent with the disaster recovery and continuity plans of the supporting installation. These contingency plans are the independent product of the end user organization, and it is the prerogative of the program manager to make arrangements in lieu of or supplementing AIS facility disaster and continuity plans as necessary to satisfy the needs of the program.

d. Identify and safeguard each plan and its related documentation in accordance with COMDTINST M5500.11, Security Manual.

2. Each commanding officer responsible for managing an AIS facility providing data processing support for essential functions shall:

a. Develop a disaster plan to allow recovery from service interruptions in a timely manner with the minimum practical impact on the users.

b. Develop a continuity of operations plan to provide reasonable data processing support should events occur that prevent normal operations at the installation.

c. Maintain an inventory of applications processed by the facility which support essential functions, adding to and deleting records from this data base upon notification from end user program managers, where applicable.

d. If the installation provides support to an essential function, thoroughly document, periodically test, and modify the disaster and continuity plans as necessary to keep pace with changing conditions.

e. Identify and safeguard each plan and its related documentation in accordance with COMDTINST M5500.11, Security Manual.

f. Address in their plan, as a minimum, the following three elements:

4.C.2. f. (1) Emergency response - Procedures to cover the appropriate emergency response to a fire, flood, civil disorder, natural disaster, bomb threat, or any other incident or activity, which will protect lives, limit damage, and minimize the impact on data processing operations.

(2) Backup operations - Backup operations procedures to ensure that essential data processing operational tasks can be conducted after disruption to the primary data processing facility. Arrangements should be made for a backup capability, including the needed files, programs, magnetic tape and paper stock, preprinted forms, etc., to operate the essential systems functions in the event of a total failure.

(3) Recovery actions - Recovery actions and procedures to facilitate the rapid restoration of a data processing facility following physical destruction, major damage, or loss of data.

3. If unplanned disruption of services would not have a critical impact on mission accomplishment, commanding officers of AIS activities shall inform the Headquarter's office, area, district, or Headquarter's unit ADPSO of that fact and a contingency plan will not be required.

**D. <u>SCOPE OF THE APPLICATION CONTINGENCY PLAN</u>.** The focus of the application contingency plan are the preparatory and emergency actions required to ensure continued availability of the essential functions of the application. The scope and depth of the plan is influenced by the activity's AIS environment, the criticality of the functional application being supported, and the user's AIS support requirement. Actions should include, as appropriate, interim manual processing requirements to achieve a minimum level of performance for extreme emergency situations and actions associated with reduced or alternate processing capability documented in the AIS Facility Contingency Plan. The contingency plan should identify:

1. Actions to be taken in advance to reduce the effect of lost or impaired service.

2. Actions required if the normal AIS environment is impaired or disrupted. The impairment or disruption can range from a few minutes to a few days depending upon the cause or situation. The contingency plan addresses this entire range as it applies to how functional requirements are met. Three situations could occur:

4.D.2. a. Limited loss of AIS capability. Impact will vary depending upon the urgency or loss potential of individual tasks.

b. Interruption to AIS operations. The duration of the interruption will depend on the time needed to restore normal operations.

c. Major damage or destruction of the facility or contents. When the activity providing AIS support becomes untenable, backup or repair of the AIS facility is necessary to restore normal operations.

3. Actions required if the AIS activity suddenly had to expand processing capability to accommodate a national emergency or some other critical event.

**E. SCOPE OF THE AIS FACILITY CONTINGENCY PLAN.** The focus of the AIS facility contingency plan are the preparatory and emergency actions required to ensure continued availability of the essential data processing requirements as determined by the requirements of application owners and end users. The scope and depth of the plan is influenced by the activity's AIS environment, the criticality of the functional application being supported, and the user's AIS support requirement. The contingency plan should identify:

1. Actions to be taken in advance to reduce the effect of lost or impaired service.

2. Actions required if the normal AIS environment is impaired or disrupted. The impairment or disruption can range from a few minutes to a few days depending upon the cause or situation. The contingency plan addresses this entire range as it applies to the activity's AIS environment. Three situations could occur:

a. Limited loss of AIS capability. Impact will vary depending upon the urgency or loss potential of individual tasks. Typical causes are:

(1) Failure of key peripheral hardware unit(s) or communication circuits.

(2) Failure of electric utilities.

(3) Loss of key application programs, preprinted forms, or documentation.

(4) Partial loss of air-conditioning.

(5) Unavailability of key personnel.

4.E.2. b. Interruption to AIS operations. The duration of the interruption will depend on the time needed to restore normal operations. Typical causes are:

(1) Failure of major AIS hardware unit(s) or air-conditioning unit.

(2) Failure of electric utilities.

(3) Fire, flood, or sabotage in or near the AIS operating environment.

(4) Intrusion of smoke, dirt, or dust.

(5) Unavailability of operations personnel caused by bomb threat, etc.

c. Major damage or destruction of the facility or contents. When the activity providing AIS support becomes untenable, backup or repair of the AIS facility is necessary to restore normal operations. Typical causes are:

(1) Natural acts (earthquake, flood, tornado, lightning, etc.).

(2) Civil disorders (bombing, explosions, fire, etc.).

(3) Mechanical breakdowns (water pipe bursting, malfunction of fire suppression systems, junction box fire, etc.).

3. Actions required if the functional application or user is denied information or service. The degree to which the functional user is affected will be determined by the actual or potential delay or denial of services and time required to recover. The user and not the AIS security staff judges the impact upon a functional application or user. The user is responsible for telling the AIS activity what priority is placed on the workload. Only the functional user can determine the criticality of AIS support to operational mission accomplishment and the urgency of the requirement for AIS services.

4. Actions required if the AIS activity suddenly had to expand processing capability to accommodate a national emergency or some other critical event.

**F.** **TESTING AND EVALUATION.** Periodic testing and evaluation of contingency plans help ensure their success should they have to be implemented. Contingency plan tests and evaluations should be made at a frequency commensurate with the risk and magnitude of loss or harm that could result from disruption of data processing support; normally, at least annually. Testing can be as extensive as transferring the entire AIS operation to an off-site facility or as minimal as conducting a fire alarm test. The depth and scope of the operational testing is dependent upon the practicality and importance of demonstrating that the plan works. Those testing the contingency plan should note that the plan addresses not only how to recover from a power loss, but also what to do if the AIS operation is destroyed. To account for the broad range of emergencies and disruptions, the team should develop scenarios, control and evaluate the test of these scenarios, and evaluate the results. This evaluation provides insight into improving the contingency plan. The contingency plan, the test plan, and the test results contribute to ensuring that AIS operations can be continued under abnormal situations and that there is adequate AIS security.

**G.** **MODEL CONTINGENCY PLANS.** Commandant (G-TDS) will provide model contingency plans for the mainframe and minicomputer environments and standard terminal environment. The model plans provide a basic outline and generic text and forms which may be used in the development of local contingency plans. The model contingency plans are provided on standard terminal floppy disks.

Contingency plans for essential functional applications will vary widely depending on the nature of the function and the data processing support thus making model plans meaningless. Commandant (G-TDS) can assist program managers and end users developing these plans by discussing various alternatives to meet requirements.

**CHAPTER** 5. PHYSICAL SECURITY

**A. GENERAL.**

1. Physical security and environmental controls shall be used to provide an acceptable level of security against potential threats, identified by risk analyses, to AIS operations. Physical security is required for spaces in which the AIS equipment is located, vital support areas, media libraries, administrative areas in which sensitive input and output is handled, remote terminal locations, areas in which portable terminals are used or stored, and other areas in which risk to the system, data, or operations may occur. Commandant (G-OIS) establishes physical security policy and procedure; see COMDTINST M5500.11, Security Manual for related guidance.

2. The great number and diversity of automated systems and installations within the Coast Guard make it inappropriate to establish universal, physical security standards. An acceptable physical security environment shall be achieved through the implementation of the following basic physical security requirements.

   a. Positive physical access controls shall be established to detect and, if possible, prevent unauthorized entry into the AIS facility and other critical areas which support or affect the operation of AIS equipment or the processing of data by the equipment.

   b. Physical access to data files and media libraries shall be limited to individuals who require access in the performance of their official duties.

   c. The effects of all types of natural disasters, such as fire and floods, shall be prevented, controlled, or minimized to the extent economically feasible by the use of detection, extinguishing systems, and well conceived and tested contingency plans.

3. Physical security and environmental controls shall be consistent with requirements and guidance contained in the Federal Information Resources Management Regulation (FIRMR) Part 201-7, Security of Information Resource Systems; the Federal Property Management Regulations (FPMR) Part 101-20; and the National Fire Prevention and Control Administration's Handbook RP-1, Standard Practice for the Fire Protection of Essential Electronic Equipment Operations; and applicable local building codes.

5.A.4. Additional physical security and environmental control requirements for automated systems which process classified information are provided in Chapter 18, Classified Information Processing.

**B. SITE SELECTION AND DESIGN CONSIDERATIONS.** The following factors shall be considered in AIS facility site selection and design.

1. Incorporate into the initial facility design provisions for controlling access.

2. Avoid sites below ground or other locations subject to flooding.

3. Keep windows to a minimum due to the risk of forced entry.

4. Avoid locations within a building that are easily accessible to the general public.

5. Select interior locations when feasible to use inherent protection of the outer building. The environment immediately above, below, and adjacent to the facility must also be considered.

6. Provide for appropriate protection of related support and operational areas located outside the central facility.

**C. ROOM CONSTRUCTION AND DESIGN STANDARDS.** The physical security of an AIS facility depends to a large extent upon the adequacy of the construction of the structure in which it is housed. The following physical security construction standards shall be used for AIS installations (computer hardware, software, and related peripherals) whose aggregate total cost exceeds $250,000 and shall be considered for those system installations of lesser value.

1. Walls. Walls shall be constructed:

   a. Solidly, and extending from true floor to true ceiling.

   b. With at least a one-hour fire rating (includes true floor and true ceiling), and

   c. Without windows, when practicable.

5.C.2. Windows. When windows in an AIS facility or vital support area are deemed necessary, they shall be protected as follows:

a. When practicable, ground floor windows should be fitted with firmly secured glass blocks or impact resistant plastic panes.

b. If glass panes are used for ground floor windows they shall be suitably barred or alarmed.

c. Windows above ground level shall be protected commensurate with the risk of the window location; e.g., height above ground, proximity to fire escapes and adjacent roofs, etc.

3. Vents and Openings. The structure shall not include any unsecured vents or openings through which entry may be gained.

4. Physical Access Controls.

a. Doors. Exterior and interior doors shall be of sufficient strength and installation to prevent unauthorized entry into the facility and shall be hinged to prevent their removal. Emergency exits shall be secured from the inside and shall be equipped with panic-type hardware.

b. Access Control System. Doors shall be equipped with a proprietary lock (e.g., Best lock). Employee entrances shall be equipped with a cypher lock or electrically released lock (e.g., card access system) to prevent unauthorized entry.

5. Instrusion Detection System. An intrusion detection system that provides a remote alarm to a manned security or response station shall be installed to detect unauthorized off-duty entrance to the space.

6. Utility Systems. In designing utility systems for AIS facilities, special attention shall be given to the following factors:

a. Electrical conduits, including lightning rods, must be placed where they will not endanger data on magnetic tapes in use in the computer area or stored in the media library.

5.C.6. b. Pipes for fluids must be located where leakage into electrical equipment will be minimized.

c. Air conditioning systems for AIS equipment temperature controls must be equipped with fire dampers to retard spreading of fire or introduction of chemical agents or smoke into the equipment area.

d. Lead-ins and shut-offs for utilities vital to the facility operations must be located with minimum exposure to possible tampering.

e. Communications lines associated with AIS operations shall be protected.

7. Construction Materials For Fire Resistance. Materials used in AIS facilities for walls, floors, partitions, acoustical treatment, raised floors and supports, suspended ceiling or other construction in the equipment room shall have a National Fire Protection Association flame spreading rating of 25 or less.

8. Fire Detection and Extinguishing Systems. Effective fire detection and appropriate fire extinguishing systems shall be included in the design of each AIS facility. See additional guidance provide below.

9. Planning Protection Against Water Damage. Below ground or basement sites are particularly vulnerable to flooding from backed up sewer lines, broken water mains, heavy rains, swollen streams. If such a site is used, provisions shall be made for drains, pumps, and emergency power for pumps, and barriers to divert flood waters from the facility, sealing walls and floors against water seepage or other protection measures determined to be applicable to the facility. In addition, no matter where the computer facility is located, a fire on the floor above will generally result in excessive build-up of weight and water that may produce leakage into the facility. The use of drains, bunkers, and channels should be considered to alleviate potential problems of this nature. Floor-to-floor integrity designed into buildings is often lost by drilling holes for utilities. These holes should be sealed to prevent their use as a path for fire or water.

**D. PROTECTION OF AIS SUPPORT AREAS.** AIS facilities depend upon the continued availability of various utilities and the use of other support areas to stay in operation. Since the source of utilities to the facility may be in other structures or areas (e.g., power transformer, emergency generators) appropriate physical security controls for these resources must be planned. When on-line AIS equipment is housed in separate structures, these structures require comparable protection.

1. Utility rooms (e.g., electrical closets, transformer vaults, air conditioning rooms, etc.) shall be equipped with proprietary locks.

2. Separate structures housing essential utility sources shall be of adequate construction to preclude unauthorized entry, including solid construction doors equipped with proprietary locks, and protected hinges, windows or other potential entry openings appropriately barred or screened, and alarm systems to detect unauthorized entry.

3. Communications terminal boards and associated equipment related to AIS teleprocessing shall be in controlled access rooms with proprietary locks.

**E. PROTECTION OF AIS ADMINISTRATIVE AREAS.** AIS administrative areas are those areas associated with an AIS activity which do not house AIS equipment. The physical security considerations for such areas will vary considerably and the protective measures used will depend upon the determination made by management in light of the sensitivity of the data involved. Consideration shall be given to:

1. Extent to which access to the area needs to be controlled while the materials are being handled.

2. Measures needed to protect the data concerned while the area is unattended, and

3. Measures needed to compartmentalize (separation of duties) the AIS related administrative functions.

**F. PROTECTION OF REMOTE TERMINALS AND MOBILE EQUIPMENT.**

1. Remote Terminals. AIS operations usually require use of remote terminal. Because of location, such terminals are especially vulnerable to misuse. Control systems shall provide for systems disconnect of the terminals when not under the immediate control of an authorized user, and shall require authentication of the user. Physical

5.F.1. (cont'd) security controls are necessary to protect the terminals from tampering and to supplement the security provided by the control system.

a. Terminal Location. Remote terminals shall be located in a room or area which shall be locked when the terminal is not under the immediate surveillance of an authorized user.

b. Disconnect Locks. To disable a terminal when unattended, it may be equipped with a disconnect lock, with properly controlled keys.

2. Portable Terminals. Management officials authorizing use of this equipment shall be responsible for assuring proper use of the equipment and for its being properly protected. This equipment shall be used only in areas in which sensitive data will not be exposed to unauthorized individuals. This equipment shall be stored in controlled space secured with a proprietary locking system when not in use. Removal of this equipment from Coast Guard buildings or spaces is subject to property removal controls. In addition, a checkout log shall be maintained for this equipment which shows to whom the equipment is checked out, purpose for which its outside use is authorized, data and time of removal and date and time of return. Users under these conditions shall assure that sensitive data and authenticators are not compromised by such use.

3. Mobile AIS Equipment. Mobile AIS equipment, i.e., on board ships, aircraft, used in support of Coast Guard missions must be used and safeguarded in a manner which will protect the Coast Guard's interests. The cognizant security element shall be consulted for appropriate guidance on the security of the equipment and the data concerned.

**G. PROTECTION OF AIS MEDIA LIBRARIES**. AIS data storage libraries for magnetic tapes, disc packs, floppy disks, or any other pertinent media shall be protected in accordance with the sensitivity of the information stored therein and its importance to Coast Guard missions.

1. AIS Media Library Construction. Media libraries shall meet the construction standards prescribed above for AIS facilities.

5.G.2. Supplemental Protection for Sensitive (Unclassified) Media. When circumstances warrant, sensitive data should be given additional protection, such as being stored in locked containers within the media library when a limited quantity of the media includes such data. When the quantity is extensive, it may be more practical to upgrade the security of the complete AIS media library by use of high security doors, sensor alarms, guard checks and other appropriate measures.

**H. DESTRUCTION OF SENSITIVE AIS MATERIALS AND WASTE.**

1. AIS Input/Output and Waste Materials which contain sensitive information may be destroyed by any means which assure that the sensitive data cannot be retrieved. The method of destruction shall depend upon the sensitivity of the data, destruction resources available, and the volume of materials. Cognizant security personnel should be consulted on destruction methods such as shredding, pulverizing, burning, etc.

2. User offices furnished computer-generated reports shall be responsible for determining what reports and input documents they hold contain sensitive data which requires destruction.

3. AIS Facility Managers shall be responsible for protection, disposal, or destruction of input documents, computer-generated products, and AIS related materials which they hold. The application system manager shall have the responsibility for advising the AIS facility manger as to the sensitivity and specific disposal actions to be taken with each identifiable item.

4. AIS-Related Materials which contain no sensitive information may be disposed of by any means the holder deems appropriate.

**I. PROTECTION AGAINST MAGNETISM EFFECTS.** Possible damage to AIS magnetic storage media can result from its exposure to magnetic forces, either fro deliberate attempts to damage the stored data or from inadvertent placing of the media too close to electrical currents capable of demagnetizing it. To minimize the danger, AIS magnetic storage media shall be kept at least twenty (20) inches from storage room exterior walls, from high voltage circuits and from lightening discharge conduits.

**J. PROTECTION OF ESSENTIAL AIS OPERATING RECORDS.** AIS facility mangers shall provide for appropriate protection of all AIS operating records which are essential to the continuity of operations or for the recovery of operations following and emergency stoppage. Suitable off-site storage shall be provided for back-up records for use in event of natural or malicious destruction of such records at the facility.

**K. PROTECTION OF SENSITIVE AIS RECORDS IN TRANSIT.** Coast Guard offices transmitting sensitive AIS records between facilities by mail or messenger are responsible for assuring that the materials are properly protected while in transit, including proper packaging, controlling, and addressing. They shall maintain controls to assure that all transmitted materials are received by addressees.

**L. ENVIRONMENTAL SECURITY.** AIS equipment, media and related utilities are highly sensitive to damage and disruption by fires that may occur in the equipment room, media storage libraries or other areas vital to the functioning of a computer system. The resulting disruption of operations, loss of vital records and the possible effects upon the mission necessitate the inclusion of fire safety as a key element of an AIS facility physical security program. The degree of environmental protection required varies from one facility to another. Such factors as the value of the equipment, operational requirements for uninterrupted system availability, local site considerations, and the uniqueness and resulting difficulty in replacing system components will influence the amount of resources committed to ensure that an adequate level of environmental security is provided. The following standards shall be used for AIS installations (computer hardware, software, and related peripherals) whose aggregate total cost exceeds $250,000 and shall be considered for those system installations of lesser value.

1. Fire protection codes and standards. Adequate fire protection for AIS equipment is achieved through a combination of minimizing the exposure to fire damage, assuring prompt detection, and providing adequate means to extinguish the fire. Commanding officers of AIS activities shall ensure AIS facilities conform to the standards contained in the National Fire Code, Volume 7, specifically the National Fire Protection Association (NFPA) Code No. 75, "Standard for the Protection of Electronic Computer/Data Processing Equipment"; NFPA 72, "Automatic Fire Detectors"; NFPA 80, "Fire Doors and Windows"; and NFPA 70, "National Electrical Code." AIS facilities shall also comply with appropriate Coast Guard and OSHA Occupational Safety and Health standards regarding the design and implementation of local fire protection systems.

5.L.2. Computer room fire prevention. Fire prevention is heavily dependent upon the physical characteristics of the area housing the equipment. Experience has shown that fires are more likely to start in adjacent offices or rooms (rather than in the facility itself), and then spread to the data processing area. Adjacent spaces should also be considered when planning a fire protection system.

a. Facility construction. All materials used in the construction of computer rooms or related facilities, to include those composing walls, floors, partitions, finish, acoustical treatment, raised floors, raised floor support, and suspended ceiling, shall have an NPFA flame-spreading rate of 25 or less.

b. Operational practices. Within the facility, good housekeeping and operating procedures are essential to maintaining a noncombustible environment. Lint from moving paper and cards ignites very easily and burns rapidly. The space under raised floors collects lint and should be cleaned regularly. Paper stocks and magnetic tapes, other than small quantities for immediate use, should not be stored in the main computer room or in auxiliary AIS equipment rooms.

c. Power-off controls. The power-off controls for the electrical system shall disconnect the ventilation system serving the computer equipment room and the power to all electric equipment in the room, except lighting. Disconnecting devices shall be placed at locations readily accessible to operating personnel, preferably at designated exit doors. These devices shall be covered to prevent inadvertent or accidental operation.

d. Smoke exhaust. Computer equipment rooms should be equipped with a smoke exhaust capability to minimize possible hazard to personnel, equipment, and storage media. Air conditioning systems should be equipped with dampers to prevent the spread of fire, smoke, and chemical agents.

3. Computer room fire detection systems. Prompt detection is a major factor in minimizing fire damage to an AIS facility. Facilities housing essential equipment shall be equipped with fire detection equipment which detects the by-products of combustion. Consideration should be given to locating detection sensors in rooms or areas adjacent, above, or below a computer equipment room where

5.L.3. (cont'd) a significant danger of fire exists. Detection systems should be specifically engineered for each AIS facility; however, the following detection system design characteristics are desirable:

a. Detectors should be located so as to detect equipment fires as early as possible.

b. The detection system should be capable of indicating the area of the room where the potential fire exists. This will permit rapid inspection of the area by computer room personnel before further unnecessary or expensive action is initiated.

c. An alarm should be connected to a monitor panel within the center and at a continuously manned guard or fire station, particularly, if the facility is sometimes unmanned.

d. Alarm systems, particularly those which are designed to activate quenching systems, should be equipped with a delay feature that will permit inspection of the possible trouble area and evacuation of the room before extinguishing agents are released.

e. The detection systems shall be designed and installed so that it cannot be easily deactivated, either maliciously or accidentally. Assistance of a fire marshal, or local fire department, should be obtained during the planning, design, and installation of a fire detection system.

4. Computer room fire extinguishing measures. The type of fire extinguishing equipment utilized will vary in accordance with the physical characteristics of the facility, the mission (sensitivity) of the computer system, and the value of the equipment and data. A minimum degree of fire protection shall be provided by hand-held extinguishing equipment and additional protection shall be provided by an area extinguishing system, as determined by risk assessment.

a. Portable firefighting equipment. Fire extinguishing equipment shall be immediately available for use in controlling fires in a computer equipment area. A carbon dioxide or halon fire extinguisher of at least 15-pound capacity shall be available for use on electrical fires. Water type fire extinguishers shall be available for use on non-electrical fires. Extinguishers shall not be located further than 50 feet from any piece of computer equipment. The

5.L.4. a. (cont'd) location and usage (i.e., water or electrical) of the extinguishers shall be indicated through the use of clearly recognizable signs posted high enough on the wall over the extinguisher so as to be visible from any point in the room. Suction devices for removing raised floor panels shall be available at each extinguisher location, if appropriate. Hand-held extinguishing equipment shall be marked to indicate the type of fire for which it is intended. Periodic training, (not less than once a year) shall be given all computer room personnel on the safe and appropriate operation of all extinguishing equipment installed at each AIS facility.

b. Area extinguishing systems. The two primary agents used in area extinguishing systems are water and halon. Water systems are generally used to limit damage to the facility itself, but, by their nature, pose a significant threat to AIS equipment. Halon systems, while more expensive, protect both the facility and the equipment from extensive damage. The relative advantages and disadvantages of water sprinkler systems and halon volumetric deluge systems must be weighed against cost, computer room construction characteristics, and operational recovery requirements. The use of carbon dioxide (CO2) systems is discouraged since they represent a significant life safety hazard. If one or a combination of the conditions listed below is present at computer installations, an area or volume flooding extinguishing system should be used to supplement hand-held extinguishers:

(1) If the construction of the computer room contains any combustible material not meeting the flame spreading rating cited above.

(2) If a significant amount of combustible material is used or stored within the computer room.

(3) If the system is operated in real time to support a critical Coast Guard mission.

(4) Where unique local conditions warrant the additional protection afforded by an area extinguishing system.

5.L.4. c. Fire drills and other related training. Managers of AIS facilities shall assure that orientation and training classes are held periodically to enable personnel who work in or around a computer room to become familiar with facility fire emergency equipment and procedures.

5. Fire protection of data storage areas. Because data storage media will sustain combustion they represent a different type of fire hazard. Also, magnetic tapes, tape reels, and disk pack containers become distorted and unusable at temperatures above 150 F. Because of this greater sensitivity to heat, the walls, floors, and ceilings of a storage area should have a 2-hour fire rating. The most commonly used means of protecting storage media is by a water sprinkler system. The temperature setting of the heads initiates operation before any major damage is done to storage media. When this type of extinguishing system is used, sufficient drains must be placed in the floor to prevent unnecessary water collection in the affected are. Carbon dioxide and Halon 1301 systems are equally suitable for use in data storage areas. An appropriate number of portable fire extinguishers should also be placed in these areas.

6. Protection of computer supplies. Computer supplies are the most combustible material used in a data processing facility. As few paper, ribbons, and chemical supplies as possible should be stored in the computer facility itself. A central storage location which is as fire resistant as practical should be utilized. This area should be equipped with suitable fire alarms and extinguishing systems, if deemed appropriate, after considering value, criticality to operation, and proximity to the computer facility.

7. Protection against water damage. Plastic sheeting should be available to protect vital pieces of equipment from damage by water from water sprinkler systems or leakage. Equipment must be powered down when water or high humidity is present. Plastic covers should be removed promptly when no longer required to prevent excessive heat built-up.

8. Local fire or police assistance. The district safety officer of each AIS installation should assure that adequate procedures have been established to obtain firefighting assistance from the appropriate local fire departments. This shall include provisions for adequate alarm and communication procedures, and ensuring computer room personnel are familiar with fire contingency plans

5.L.8. (cont'd) and necessary actions in the event of a fire. Local fire department and district safety office personnel should be invited to visit the facility, review the fire protection system being utilized, and discuss with appropriate personnel, matters involving fire protection of the computer facility. Local law enforcement agencies should also be contacted to review plans for providing support in the event of riot or other civil emergencies where they may be called upon to prevent disruption of essential data processing activities at the facility.

## CHAPTER 6. PERSONNEL SECURITY

**A. GENERAL.** Personnel are generally considered to be the most significant threat to an automated information system; thus the selection of reliable and trustworthy personnel is a major factor in achieving AIS security. Personnel hiring and placement practices should ensure that each individual who is involved with an AIS has a high level of competence, loyalty, and integrity. The demands for competence, loyalty, and integrity may vary depending on the sensitivity of the system and the nature of the individual's responsibilities.

**B. SCOPE.** This chapter identifies the criteria to be used within the Coast Guard for positions directly or indirectly associated with an AIS. This chapter highlights criteria relative to responsibilities associated with AIS. The criteria apply to any position, regardless of civilian classification series or grade having access to an automated system. Additional guidance is contained in COMDTINST 5510.10, Civilian Personnel Security Program and COMDTINST M5510.16, Military Personnel Security Program.

**C. DISCUSSION.**

1. The Office of Management and Budget (OMB) Circular A-130 established position sensitivity standards for personnel associated with AIS. Federal Personnel Manual (FPM), Chapter 732, Subchapter 2, dated January 6, 1984 established four levels of sensitivity for ADP positions. DOT Order 1630.5 implements the FPM guidance for the department. Four categories have been established for designating computer and computer-related positions. They are Automated Data Processing (ADP) IV, III, II, and I which are comparable to the personnel security requirements identified as Special Sensitive, Critical Sensitive, Noncritical Sensitive, and Nonsensitive, respectively. Application of the criteria for designating category levels of individual positions normally does not fit a precise formula. A determination must be made on the basis of judgment, considering numerous factors, including:

    a. The degree of supervision or review afforded the occupant of the position.

    b. The extent of AIS security and protective measures in effect.

    c. The sensitivity of the data being processed.

    d. The degree to which the data being processed is accessible by individuals through outside terminals.

6.C.1. e. The extent to which the activities associated with the position are performed in isolation from concurrent processes.

f. The extent to which responsibility for violations or attempted violations of AIS security can be established.

g. The degree of accessibility to other data in a system through intrusion by telecommunications or time-sharing.

**D. FPM CRITERIA FOR DESIGNATING POSITIONS.** Specific criteria for assigning positions to one of the ADP-IV, ADP-III, ADP-II and ADP-I categories include:

1. ADP-IV (Special Sensitive) - Includes any position which the agency head determines to be at a level higher than Critical Sensitive based on one of the following criteria:

a. The greater degree of damage that an individual by virtue of occupancy of the position could effect to the national security.

b. Special requirements concerning the position under authority other than Executive Order 10450, Security Requirements for Government Employees, such as DCID 114, Director of Central Intelligence Directive.

c. Any position determined to impose a risk in terms of AIS security above that of the critical-sensitive level.

2. ADP-III (Critical Sensitive) - Includes any position in which the incumbent:

a. Has access to Top Secret National Security defense information.

b. Is responsible for the planning, direction, and implementation of a computer security program;

c. Has major responsibility for the direction, planning, and design of a computer system, including the hardware and software;

d. Can access a system during the operation or maintenance in such a way, and with relatively high risk for causing grave damage or realize a significant personal gain.

6.D.2. Such positions may involve:

a. Responsibility for the development and administration of agency computer security programs, and also including the direction and control of risk analysis and/or threat assessments.

b. Significant involvement in life or mission critical systems.

c. Responsibility for the preparation or approval of data for input into a system which does not necessarily involve personal access to the system, but with a relatively high risk for effecting grave damage or realizing significant personal gain.

d. Relatively high risk assignments associated with or directly involving the accounting, disbursement, or authorization for disbursement from systems of:

(1) dollar amounts of $10 million per year or greater, or

(2) lesser amounts if the activities of the individual are not subject to technical review by higher authority at the Critical-Sensitive level to insure the integrity of the system.

e. Positions involving major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring, and/or management of systems hardware and software.

f. Other positions designated by the agency head that involve relatively high risk for effecting grave damage or realizing significant personal gain.

3. ADP-II (Noncritical Sensitive) - Includes any position in which the incumbent is responsible for the direction, planning, design, operation, or maintenance of a computer system, and whose work is technically reviewed by a higher authority at the Critical Sensitive level to insure the integrity of the system. Such positions may involve:

a. Access to Secret or Confidential national security materials, information, etc.

6.D.3. b. Responsibility for systems design, operation, testing, maintenance, and/or monitoring that is carried out under technical review of higher authority at the Critical Sensitive level, to insure the integrity of the system. This level includes, but is not limited to:

(1) Access to and/or processing of proprietary data, information requiring protection under the Privacy Act of 1974, and Government developed privileged information involving the award of a contracts.

(2) Accounting, disbursement, or authorization for disbursement from systems of dollar amounts less than $10 million per year.

c. Other positions as designated by the agency head that involve a degree of access to a system that creates a significant potential for damage or personal gain less than that in Critical Sensitive positions.

4. ADP-I (Nonsensitive positions) - Includes all ADP computer positions not falling into one of the above sensitive positions.

| **E. APPLICATION OF CRITERIA**. The designation of position
| categories should normally follow a risk assessment for the
| AIS in question. Contact Commandant (G-OIS) if assistance is
| needed in determining position sensitivity catagory.

**F. INVESTIGATION REQUIREMENTS**. All Coast Guard and contractor personnel employed in positions designated as ADP positions (ADP-I through ADP-IV) must undergo an investigation in accordance with FPM Chapter 732 and receive proper clearance if classified information is processed. The scope and comprehensiveness of the investigation is based on the sensitivity of the position. Investigations and clearances must be performed prior to performance of duty unless a specific waiver is granted by Commandant (G-OIS).

## CHAPTER 7. ADMINISTRATIVE SECURITY

### A. GENERAL.

1. Administrative security consists of management constraints, standard operational security procedures, security accountability controls, and those additional administrative actions necessary to protect AIS resources. Administrative security controls define who, what, where, when, how, and how often actions are taken in the work flow process to ensure the integrity and confidentiality of AIS resources. It is at those points in the process where control passes from one function, element, or individual to another, that control can be lost.

2. The control principles described in this chapter apply to software development and maintenance activities as well as data processing "operations." Control of software during the development and maintenance processes are as important to the overall security of operations as control over the central processor.

3. Each AIS activity shall prescribe administrative security requirements in the form of an AIS security standard operating procedure (SOP) to guide the actions of programmers, equipment operators, and other data processing specialists. Specific requirements shall be based on the security threats identified by the risk analysis conducted for the system or facility and the administrative controls described in this chapter. The SOP may be included as part of a command instruction or the Activity AIS Security Plan. The SOP shall include assignment of responsibility for assuring awareness of all employees concerned of the administrative security requirements, and for checking their compliance with the requirements.

4. Additional administrative control requirements for automated systems which process classified information are provided in Chapter 18, Classified Information Processing.

**B.** **MANAGEMENT CONSIDERATIONS**. The security of an AIS or facility can be no greater than the reliability and trustworthiness of its staff. Management constraints to be exercised in promoting AIS security interests include election of suitable individuals to fill AIS positions, assuring employee awareness of their security obligations, monitoring their compliance with security requirements,

7.B. (cont'd) tailoring duty assignments to reduce opportunities for security controls to be circumvented and maintaining positive controls to assure that unauthorized persons are unable to access the data.

1. Personnel Selection. Selection and retention of a reliable AIS staff is a personnel management function. Personnel security requirements, including requirements for clearances and background investigations, are prescribed in Chapter 6.

2. Training. AIS staff members must be properly trained in exercising security precautions and must be periodically checked on their compliance with established requirements.

3. Delineation of Responsibilities. Duties, privileges, responsibilities, and specific limitations of all personnel involved in the operation of a facility processing sensitive (Level II) data shall be specified in writing and periodically reviewed for adequacy by management or security personnel. All personnel actively involved in AIS (operators, programmers, analysts, and AIS management) should have their security responsibilities incorporated as a job duty/function in the Officer Support Form (OSF), Enlisted Performance System (EPS) or Critical Job Element (CJE).

4. Separation of Duties. When AIS functions are prone to manipulation (e.g., payroll, inventory control, etc.) duty assignments should be made so that one individual does not exercise complete control over the entire AIS function. This not only provides a balance against possible fraud, but also assists in checking for errors.

5. Supervision. AIS staff members must be sufficiently supervised to assure that they maintain and adequate level of competence in applying the specified security controls. Supervisors shall appropriately limit access to AIS equipment and data by employees who are inadequately trained or whose reliability and trustworthiness has not been established. Supervisors need to be particularly alert to potential threats to the system posed by employees who are the subject of adverse personnel actions or whose trustworthiness has become questionable.

6. Misuse of Functions and Privileges. Coast Guard employees or other individuals authorized access to a Coast Guard computer system who knowingly misuse or abuse a system shall be subject to disciplinary actions as well as any criminal penalties which may result from data alteration, system misuse, or diversion of system resources for personal gain or profit.

7.B.7. Protection Against Disgruntled Employees. Employees, who are about to be discharged or against whom adverse action is being taken, are a threat to destroy equipment or data files, modify them for their personal benefit, or commit other hostile acts. Administrative procedures should be in place to promptly and completely terminate access to AIS resources by disgruntled and disaffected personnel. The use of administrative leave should be considered as an avenue of removing the potentially disruptive and dangerous threat of personnel being separated for cause.

**C. IDENTIFICATION OF SENSITIVE INFORMATION.** The administrative controls required for an AIS depend on the value of AIS assets, including the sensitivity of the information processed. The organizational component (user) requiring data processing support is responsible for identifying those applications which process sensitive information. Specific responsibilities include:

1. AIS users shall notify the ADPSO or ADPSSO that sensitive information is to be processed, accessed, or requested.

2. Each ADPSO or ADPSSO shall maintain a list of sensitive applications processed by the AIS installation. This inventory shall include the application program name, identifier, user(s), and an indication of the sensitivity of the information processed (e.g., Privacy Act, FOUO).

3. The ADPSO or ADPSSO shall inform the AIS installation manager of all applications that process and/or access sensitive information and shall advise him of the security controls appropriate for his processing environment.

4. AIS users shall adhere to the Federal Register publication requirements for a system of records subject to the Privacy Act and observe the appropriate waiting period prior to requesting that such information be processed or accessed by an AIS.

**D.** **CONTROL OF ACCESS TO AIS AREAS.** AIS areas are those in which AIS equipment is located, vital support areas, AIS media libraries, remote terminal locations, administrative areas in which sensitive AIS data or systems control records are being processed, and similar locations. Appropriate management controls must be established to specify who is authorized to have access into the AIS area, to positively identify the authorized individuals and to exclude those who do not have authorization. Provisions must be made for admitting maintenance personnel and other appropriate individuals into the AIS area under conditions which do not permit them to

7. D. (cont'd) have access to the data or to interfere with the AIS operations. The AIS security SOP should prescribe how access is to be controlled and who is responsible for assuring that the controls are applied.

1. Administrative Access Controls. Management controls and procedures shall be established to supplement the physical security measures implemented to restrict access to essential computer equipment and support areas. These controls should specify who is to have access to what areas, what identification, if any beyond personal recognition, is required and who shall be responsible for granting access to visitors and maintenance personnel. Additional access control requirements for AIS media storage areas are specified below. Access controls shall address both duty and non-duty hours.

2. Designation as a Limited Access Area. AIS areas (e.g., computer rooms, tape libraries, output distribution areas) that process or store sensitive information shall be designated as a **"limited access area,"** however, exterior signs indicating such are not required unless the facility is located in a place which invites unauthorized and unescorted traffic. Entry to these areas shall be restricted to those personnel with a valid requirement and authorization to enter.

3. Authorized Individuals. Lists of authorized individuals, updated as required, should be provided to those responsible for exercising access controls. Such lists should identify those who need full access to the AIS area, those who are to be admitted for maintenance or other specified repetitive purposes, etc.

4. Personal Identification. Positive personal identification shall be required for access to AIS areas.

5. Excluding Unauthorized Individuals. Normal physical security measures such as locking of entrances or placing a receptionist at unlocked entrances to an AIS facility should provide proper screening. Locked doors may be equipped with proprietary locks to which only authorized individuals have keys or cipher combinations. Access to limited areas within an AIS facility can also be controlled in the same manner.

7.D.6. Visitors. Visitors to the AIS areas shall be subject to appropriate screening measures which identify to the proper authority the visitor's identify and purpose of the desired visit. If the visit is approved, the visitor shall be escorted or kept under surveillance during the visit. Visitor sign-in/sign-out registers shall be maintained.

7. Security of AIS equipment room(s) during non-operational hours. All equipment rooms shall be secured upon the completion of the duty day or at any other time the facility is unoccupied, such as during a fire drill, bomb threat, etc. Strict accountability will be maintained over keys, combinations, or identification numbers which permit access to the facility. A security survey, risk assessment, or audit may disclose vulnerabilities of the facility in the after-hours environment. These may include entry into the computer room through an overhead crawl space, beneath raised flooring which extends beyond the controlled area of the equipment room, or through air conditioning vents or ducts. During non-duty hours, computer facilities processing sensitive information shall have entrances protected by a minimum of two separate, independent barrier/other security systems.

8. Controlling Access to Remote Terminals and Portable Computers. Administrative procedures to control access to AIS areas in which remote terminal devices and portable computers are located must be provided to supplement hardware/software features used to limit use of the devices. The AIS areas shall be locked when unattended to safeguard against theft, damage, or misuse of the equipment.

**E. OPERATIONAL PROCEDURES.** Good AIS operating practices and procedures provide controls which protect data from accidental or unauthorized modification, destruction, or disclosure during input, processing, or output operations. The following controls shall be considered and incorporated in the SOP where practicable.

1. Control of Work Flow. Positive control of both automated and manual processing shall be provided for those activities processing sensitive information. Controls should be detailed and explicit, especially when passing from function to function, so that historical documentation of such handling may be used as the basis for internal review and audit. The following procedures are intended to provide security for sensitive operations and should be used where appropriate.

7.E.1. a. Control documents. Each request for service or job submitted by a user should be verifiable through the use of ID numbers or passwords assigned to authorized users, prior to acceptance. Once accepted, the job should be controlled by means of a single control document containing such pertinent information as identification of the submitter, processing to be performed, control or transaction totals, classification and sensitivity of processing, program and file requirements, run time, output verification instructions and distribution. This control document should identify all procedural requirements and be verified by supervisory personnel at major functional transfer points (e.g., upon receipt and logging, when scheduled for production, when programs and files are identified and withdrawn from the library, when passed to operations).

b. Input/output control. An input/output control group should be established to screen materials and control their transfer between external activities and internal operations. All material entering and leaving the facility (hardcopy printouts, magnetic tape reels, card decks) should pass through this control group for review prior to release. Functions performed during input/output control should include: receipts for input; preparing the master control document; recording of document counts and control totals; initiation of corrective action on improper inputs; submitting source documents to data preparation; checking results of data validation runs; identification of library requirements (tapes, disks); submitting jobs to operations for processing; receipts for output; reviewing process accounting data to verify counts, hash totals, and reasonableness of processing time; reviewing output for processing errors, proper security markings, and caution statements, if required, approving release of materials.

c. Scheduling and job control. Well-defined procedures for scheduling, processing, and verifying job control instructions are essential to the security of sensitive operations.

(1) Scheduling. Whether manual or automated, job scheduling activities define the data, programs, and system components to be interacting during any given period of processing. Effective procedures should specifically identify job

7.E.1. c. (1) (cont'd) classes by security classification and degree of cumulative as well as individual sensitivity, in addition to the various types of resources required.

(2) Job control. To ensure adequate control, job execution instructions should be well detailed (run time, dependent jobs, core requirements, input/output devices). Job control or command language capabilities and instructions should be complete and fully utilized so as to minimize need for manual intervention. Job stream controls are useful in enforcing user identifications; specifying task, storage and device requirements; and stating required responses to exceptional circumstances (e.g., execution abort, device malfunction, data errors). All job control instructions and instruction decks should be safeguarded and job streams validated by supervisory personnel prior to being passed to operations for execution.

(3) Logs. System journaling facilities and operating logs should detail systems activity, to include all runs, errors, restarts, interrupts, control instructions, and operator intervention. Operator console records, in particular, should be reviewed daily, or at the end of each shift, by supervisory personnel for indication of effectiveness of security controls. Accurate historical documentation is essential for performance audit and effective compliance determination, therefore copies of logs shall be maintained for at least 90 days.

2. Start-up, Shutdown, and System Failure Procedures.

a. System operations are especially susceptible to exploitation of vulnerabilities during both scheduled and unscheduled changes of operational state occurring during system start-up, shutdown, or failure. For this reason, operational and security controls must be intensified, enforced, and reviewed for compliance to minimize the possibility of system compromise.

b. State-of-the-art system software and control features provide for "failsoft" and automatic restart capabilities which can make system failures transparent to users and often inconsequential to

7.E.2. b. (cont'd) system operators. In systems supporting remote access resource sharing devices, susceptibility to exploitation peaks during these conditions. Such instances shall be fully documented and investigated by system security personnel for evidence of exploitation.

c. Detailed logs, records, or other documentation of operational states at the time of failure are essential in order to provide audit trails for use in analysis of system failures.

d. Frequent operational failures caused by unreliable hardware, software, or procedures create an environment within which effective security is difficult to achieve. These conditions should be corrected promptly where secure operations are required.

e. For those systems processing sensitive data, detailed procedures and checklists shall be developed which identify actions to be taken during initial start-up, scheduled shutdown, unscheduled shutdown, and restart after unscheduled shutdown to ensure system integrity. Procedures should include requirements such as load a fresh, certified copy of supervisor software, obtain approval from system security officer to commence restart sequence, protect all removable storage items, disconnect remote terminals, and observe and record all system indicators to determine causes of shutdown.

3. Magnetic Storage Media Control.

a. Identification of AIS Storage Media. Containers, tape reels, disk packs or other storage media must be positively identified to assure that the data they contain is not release in error. Intermediate (e.g., scratch tapes) and final magnetic storage media shall be marked to clearly identify their contents (e.g., "FOR OFFICIAL USE ONLY" or "FOR OFFICIAL USE ONLY-PRIVACY ACT DATA") to prevent their accidental release and to warn individuals of the need for special handling.

b. Logs. Magnetic storage media shall be controlled in a library to ensure that it does not result in unauthorized disclosure of sensitive information.

7.E.3. b. (cont'd) Accurate accounting for sensitive information shall be ensured by taking both periodic and unscheduled inventories of all files and storage media containing sensitive information. The results of such reviews and/or audits shall be documented. Additionally, extracts or working copies of existent files and/or data bases shall be similarly controlled.

c. Storage. Magnetic storage media shall be placed in either a lockable container and/or stored in a room or vault with the appropriate physical security requirements to insure it's integrity.

d. Prevention of Inadvertent Destruction. Steps shall be taken to prevent accidental erasure, over-write or destruction of AIS storage media containing essential data such as master files or system programming. Specific operational instructions should also be established to cover such incidents as dropped disk packs, etc.

e. Media Library Controls. AIS media library procedures shall require that all pertinent media be stored in authorized locations, be properly accounted for, and be released only under prescribed conditions. Normally the only exceptions to central media library storage are when it is in use in the AIS equipment room or when it is stored remotely in an authorized location for backup purposes.

f. Control of Access to Data Storage Areas. Besides the physical security measures established for data storage areas, appropriate managerial controls must be implemented to reinforce these physical controls.

g. Magnetic Media Sanitization. Administrative controls must be implemented to prevent unauthorized individuals from obtaining sensitive data from internal memory work areas, scratch disks, and scratch tapes. Administrative procedures shall be implemented that require the overwriting of main storage memory disks or tapes following the processing of senstitive information. Magnetic tapes may also be sanitized through the use of a bulk degausser. Appropriate allowances must be made for the release of memory dumps and associated data records to the vendor's technical personnel when required for debugging or problem resolution.

7.E.3. h. Disposal of Residue Materials Containing Data. Operating procedures shall assure that any sensitive residue to be destroyed is handled in such a manner that exposure to unauthorized individuals is precluded.

4. Hardcopy Output Control.

a. Identification of Output. Output products shall be labeled "FOR OFFICIAL USE ONLY" or "FOR OFFICIAL USE ONLY-PRIVACY ACT DATA" as applicable to warn individuals of the need for appropriate handling. Any one or a combination of the following labeling methods may be used.

(1) Computer-generated page markings that conspicuously identify products as containing sensitive information.

(2) Stamps or labels.

(3) Cover sheets attached to the products that warn that the contents are subject to special handling under the Privacy Act.

b. Logs. Procedures shall be established for maintaining correct, current accounting of all human readable (e.g., english, binary, hexadecimal dumps, tape prints, etc.), senstive information in a computer facility. Similar procedures shall be maintained for each transfer of storage media containing sensitive information either to or from a computer facility (local or remote).

c. Inventories. Accurate accounting for sensitive information shall be ensured by the ADPSO taking both periodic and unscheduled inventories of all printed media containing sensitive information. The results of such reviews shall be documented.

5. Erasure of Sensitive Information.

a. Erasure of sensitive information stored on magnetic storage media shall be accomplished by either degaussing or overwriting. To preclude the unauthorized recovery of temporary sensitive information residing on magnetic storage media, one of the following actions shall be taken:

7.E.5. a. (1) Erasure of personal information.

(2) Use of a dedicated pool of magnetic storage media.

(3) Assign storage media or space therein to named individuals.

b. Sensitive information that is to be transferred on magnetic media outside of the AIS installation where it is generated, altered, or copied shall be placed on storage media that was erased prior to recording. Appropriate steps shall be taken to ensure that the media after recording, does not contain unauthorized sensitive information.

6. Waste Disposal. Paper products, such as listings, cards, paper tape, and carbons, will be disposed by burning, shredding or pulverizing. Under no circumstances will paper products be reused (e.g., re-spliced paper, scratch pads) in a form that would permit access to sensitive data.

7. Security of Operational Software. Once software has been accepted and certified for operational use, it shall be kept under close and continuous control in order to ensure that unauthorized changes are not made. For the most sensitive software, a master copy should be safeguarded and never used for actual production operations. Production copies of this software should be generated from the master copy and refreshed frequently or compared side-by-side to the master to ensure its integrity. A program library can provide the necessary control and protection of software.

8. Modification of Operational Software. Modification and maintenance of sensitive operational software shall be accomplished under rigorously controlled conditions which first validate the cause of any operational failure, the presence of any design flaws, or the new requirement necessitating change. Procedures shall be implemented so that a formalized approval and/or authorization process is followed whenever modifications are made to sensitive programs. Upon completion of maintenance or modification, independent verification of the changes shall be accomplished prior to placing software back into operational status. A record of changes made and a copy of the modification shall be maintained, preferably with a program run manual. The use of these procedures should be considered for computer programs other than sensitive programs. COMDTINST M5234.2, ADS Documentation Standards Manual provides additional guidance in this area.

7.E.9. Maintenace of Documentation. The preparation and maintenance of program documentation (see COMDTINST M5234.2, ADS Documentation Standards Manual, is important as a security measure, as well as an operational necessity. AIS managers should require, particularly with respect to programs used to process sensitive data, the secure maintenance of documents and records which fully and accurately describe the system and changes made to it. This documentation is critical when performing the sensitive application certification review. Guidance contained in the ADS Documentation Standards Manual is applicable in concept, intent, and direction to all systems, but level of detail may vary with the sensitivity and complexity of the system.

**F. AUDIT PROCEDURES.** Audit trails are designed to enable the AIS facility manager or ADPSSO to determine what actions have transpired which may affect the security operations of the system and permit supervisors or managers to review operations to determine if any abuses are occurring. To be effective, these records must determine what transactions were made, when, and in what sequence. There are two categories of audit trails, manual and automated. All procedures must be accomplished under the control and with full knowledge of the ADPSSO. Following are types of audits which, when used as mutually supportive mechanisms, will serve as the principal tools used in evaluating the security posture of an automated information system:

1. Manual/automated logs.

    a. System user access roster. A current roster maintained by the ADPSSO of all personnel authorized access to the system. This roster contains the name, grade, organization, and security clearance/special access authorization, user identification code, functional responsibilities (e.g., programmer, operator, maintenance, customer, etc.), and file access authorizations where applicable.

    b. Operational/support access roster. A record maintained of all personnel who require unescorted entry to restricted operational areas; e.g., central computer facility, tape library, remote terminal areas, etc. This record should include as a minimum, the name, grade, organization, and security clearance/access authorization of each individual requiring routine access to the area.

7.F.1. c. Visitor log. A record maintained of all visitors who require access to the restricted operational areas and who are not approved for unescorted access. This record should include the visitor's name, grade, organization, as well as the date, time entered and departed, purpose of visit, and the signature of the escort.

d. Library logs. Records used to maintain current inventory and control access to magnetic storage media maintained in the library (e.g., "sign-out" logs which list media identification, classification/sensitivity, date and time of release and return, and disposition).

e. Customer service logs. Records to control release of products/material outside the confines of the computer processing environment. Such records include names of users (organizations and designated representatives) and authorized transactions.

f. Reproduction logs. Record of what materials have been reproduced, their classification/sensitivity, by whom, for what purpose, and disposition.

2. Application Software. Automated, internal programs can be introduced on line into file-oriented systems to audit computer accesses and interactions with system programs and files. As a minimum, such programs should provide for the following:

a. System access log. A record made of the entry, identification of terminal, identification of user, time/date, time used, and input/output device dedication.

b. Protected file usage log. A record of the file being opened and closed, identification of user, activity taken against the file, and identification of terminal access to file.

c. Transmission log. A record of the identification of terminal receiving acknowledgement, identification of user request and files involved, date/time, and identification of communication port/line.

d. Secondary storage log. A record of the recorded area of memory assignment by classification/sensitivity, time area was dedicated, and time area was released.

7.E.2. e. Suspected violations log. A record of the type of suspected violation, identification of terminal, identification of user, and date/time of suspected violation.

3. Security Verification Programs. Security verification programs, or slave programs, provide continuous checks on the hardware and software security of the system's operations. Actual responses are compared to known correct responses to verify that the system is responding properly. A summary of all tests should be recorded and reviewed periodically by the ADPSSO.

**G. USER IDENTIFICATION AND AUTHENTICATION.** System controls shall be used to require that user identity be established and authenticated, and that data access is limited to that for which the user is specifically authorized. Passwords are the most common form of authentication. Biometric authentication devices may be used in addition to passwords if a risk analysis indicates the needed for increased protection.

1. Passwords. Passwords are character strings used to authenticate an identity; passwords control access to an AIS by assuring unequivocal authentication of the user's claimed identity. Knowledge of the password that is associated with a user ID is considered proof of authorization to use the capabilitities associated with that user ID.

   a. Passwords shall be handled, stored, and controlled at the level of the most sensitive data in the system. Knowledge of passwords will be limited to persons with a need-to-know. Normally, this should be one person, the user. In all cases, the ADPSO/ADPSSO shall ensure that the user holds appropriate clearances (or functional need-to-know for unclassified, sensitive applications) and has a valid operational requirement to access the system. Individuals assigned passwords are responsible for assuring that the passwords are not intentionally or inadvertently compromised. Before an initial password is issued, the individual users will be briefed on:

      (1) Password exclusiveness,

      (2) Measures for safeguarding passwords,

      (3) Prohibition against revealing to others, and

7.G.1. a. (4) Requirement to inform the ADPSO/ADPSSO immediately of any detected misuse of passwords or other practices potentially dangerous to system security.

b. In those instances where the ADPSO or ADPSSO issues passwords, user notification shall be made by direct personal contact with the individual user, whenever possible. If distance precludes direct contact with the user (e.g., remote terminal access), the ADPSSO may authorize an individual to act for him in the issuance of passwords.

c. In systems involving central issuance of passwords, a password shall be retired when the time limit on its use has expired, the user's duties no longer justify having a password (e.g., retired, discharged, or otherwise separated from the duties or function for which the password was required), or the user is no longer trusted. Passwords, as unique identifiers of individual authority and privilege, must not be allowed to migrate between individuals even though employed on the same project. Check-out sheets, if used at the command, for departing personnel should include a line item for the ADPSO/ADPSSO to ensure password retirement.

d. If overstrike or character suppression capability is not available when logging on to the system, users shall assure that passwords are not left on terminals, in desks, or with printouts or other materials to which other individuals have access.

e. Passwords can be generated by either the ADPSO, ADPSSO, or the user depending on operating conditions and command policy. Passwords shall be no less than 6 alphanumeric characters in length to minimize the risk of passwords being "guessed" by automated trial-and-error techniques. Passwords selected should be words that are not difficult to remember, but should not be based upon information readily identifiable with the individual. Passwords based on family member names, birthdays, etc. can be easily guessed and should be avoided. The recommended method for the development of a password is to take a group of words or phrases familiar to the user and combine all or portions of them to form the password. For example: the password EVOTTUPA is derived from the phrase, "EVery Other TUesday is PAyday" and can be easily memorized.

7.G.1. f. Passwords shall be changed as frequently as needed to protect their integrity, and as a minimum, at least every six months. They shall be changed whenever compromise is known or suspected.

2. Protection of Passwords. To be effective, access to passwords must be limited to those who have responsibility for using or maintaining them. Passwords shall be protected at a level commensurate with the sensitivity of data contained in the system. Passwords shall be promptly deleted from the system when the user no longer is authorized access (e.g., resignation, retirement, reassignment to other duties, etc.).

**H. REPORTING AIS MISUSE, ABUSE, AND ERRORS.** The effectiveness of the security controls prescribed for Coast Guard automated systems and support facilities depends upon the competency, integrity, and dedication of each individual concerned with system use, not only in applying the controls, but also in reporting any systems errors or abuses which come to their attention.

1. Misuse or Abuse of AIS. Most Coast Guard systems are designed for simplified system usage and for providing to the user a variety of system resources. This increases the susceptibility to misuse or abuse of the system by individuals who are not authorized to access the information or who improperly copy, alter, or destroy data or use systems resources for unauthorized purposes.

    a. Deliberate misuse or abuse of Coast Guard resources, including the use of timesharing services to which the Coast Guard subscribes, makes the individual subject to disciplinary action and criminal prosecution.

    b. Incidents of loss, theft, or damage to computer equipment, software, and data or attempts to access sensitive information by persons not properly identified or authorized shall be reported immediately to the appropriate AIS facility manager, the ADPSSO, and command security manager. The command security manager shall coordinate investigations when circumstances warrant. Commandant (G-OIS) shall be notified of all investigations in a written report; the report shall be marked "For Official Use Only." The ADPSSO shall maintain a log of all AIS related security incidents for each system he for which he is responsible.

7.H.1. c. Reporting requirements shall be communicated to Coast Guard personnel who are engaged in the operation, programming, and administration of Coast Guard computer systems, related facilities, and related activities, to include commercial time-sharing.

2. Inadvertent Receipt of Data. Input or output may be misrouted or mishandled, thus possibly resulting in unauthorized access to sensitive data. This can occur as the result of a malfunction of system hardware or software, the misrouting of data through communications lines, or human errors in distributing input or output. Individuals who inadvertently receive such data shall promptly report this fact and return the data to the appropriate system administrator or AIS facility manager. Automated system managers shall maintain a log of these events for subsequent diagnostic analysis by appropriate systems and security personnel. Corrective measures shall be initiated to eliminate the causes of misrouting of input or output materials.

3. Escape of Data from System Controls. Any authorized user of a Coast Guard system who discovers a system failure which results in the output of data to which he is not authorized shall report details of the system failure to the appropriate AIS facility manager.

## CHAPTER 8. HARDWARE SECURITY

### A. GENERAL.

1. Hardware resident architectural features are becoming an increasingly important element in the enhancement of total automated system security. Depending upon the relative age, sophistication, and design of the computer system, hardware based security controls represent an important factor that must be considered when evaluating the security environment and capabilities of an automated system. Conversely, the lack or absence of hardware embedded security features and/or the presence of known hardware architectural vulnerabilities that can be exploited by a penetrator will require the use of compensatory actions in other elements of the AIS security program.

2. Hardware controls function as part of the system itself, in contrast to the external protective measures discussed in other chapters. As AIS hardware technology becomes more sophisticated, system security will be increasingly dependent upon these controls. Administrators of operational systems and those engaged in planning and designing future automated systems should be familiar with these controls and the effect they have in enhancing the total security of a system. They shall be evaluated in the acquisition and implementation of any new AIS. The implementation of these measures may depend upon the sophistication of the computer system, the sensitivity of data processed by the system, and the presence or absence of other security factors as identified by risk assessment. This chapter discusses general guidance in this highly technical and rapidly evolving aspect of computer security.

### B. HARDWARE SECURITY POLICY.

Persons responsible for designing, developing or acquiring new systems or implementing significant modifications to existing systems which process classified or sensitive information shall use cost effective hardware security controls, or features. Funding support for retrofitting hardware security controls for existing systems not undergoing significant modifications, will be evaluated by Commandant (G-TDS).

### C. HARDWARE SECURITY FEATURES.

1. Integrity Features. Processor architecture should include certain equipment controls that are intended to assure the functional correctness and operational

8.C.1. (cont'd) reliability of the system. Such equipment features as parity characters and validity checks enhance system security, as well as provide protection against equipment malfunctions.

2. Memory and Storage Protection. Hardware controls, supplemented by system software, should be exercised by the system over the memory address to which a user program has access.

3. User Isolation. A computer system should have the capability to effectively isolate users from each other and from access to the protective controls of the operating system. The principal hardware controls that accomplish this function are base-addressing registers, bounds registers, and checking circuits that ensure that programmed memory addresses are actually limiting access to authorized programs and data. Length check register and hardware enforced storage locks also provide user isolation.

4. Supervisor/Executive Protection. Entrance to the supervisory or executive mode should be hardware controlled.

5. Identification and Authentication. Certain hardware measures can be utilized in remotely accessed computer systems to provide improved means of identifying users and/or terminal devices. These include the use of hardware generated characters that identify the terminal to the central system, and magnetically encoded badges or cards which can activate the terminal device.

**D. DESIRED HARDWARE SECURITY FEATURES**. The following features or capabilities should be included in any new automated information systems when supported by the findings of a risk assessment.

1. The execution state of a central processor should include one or more "protection state variables," which determine what instructions should be executed by the processor. For example, a processor might have a master mode/user mode protection state variable, in which certain instructions are illegal except in master mode. Modification of the protection state variables will be so constrained by the operating system and hardware that a user cannot access information for which he has no authorization.

8.D.2. The ability of a central processor to access locations in memory, including primary and auxiliary memory, should be controlled. For example, in user mode, a memory access control register might allow access only to memory locations allocated to the user by the operating system.

3. The operation of certain instructions should depend on the protection state of the central processor. For example, instructions which perform input or output operations would execute only when in master mode. Any attempt to execute an instruction which is not authorized should result in a hardware interrupt which will permit the operating system to interrupt and/or abort the program containing the illegal instruction.

4. All possible operation codes with all possible tags or modifiers, whether legal or not, should produce known responses by the computer.

5. All registers should be capable of protecting their contents by error detection or redundancy checks. These include those which set protection state variables, control input or output operations, execute instructions, or which are otherwise fundamental to the secure operation of the hardware.

6. The contents of any register which can be loaded by the operating system should also be storable, so as to permit the operating system to check its current value against its presumed value. (The term "register" as used in this enclosure refers primarily to index or general purpose registers, rather than an isolated address of a single storage location within the computer.)

7. Error detection should be performed on each fetch cycle of an instruction and its operand (e.g., parity check and address bounds check).

8. Error detection (e.g., parity checks) and memory bounds checking should be performed on transfers of data between memory and storage devices or terminals.

9. Automatic programmed interrupts should function so as to control system malfunctions and operator errors.

10. The ability to identify remote terminals for input or output should be a feature of hardware in combination with the operating system.

8.D.11. Read, write, and execute access rights of the user should be verified on each fetch cycle of an instruction and its operand.

12. Processor architecture should include certain equipment controls to ensure correctness and operational reliability of the system. Such integrity features as parity characters and validity checks and enhance system security, as well as provide protection against equipment malfunctions.

13. Memory and storage protection, implemented through hardware controls and supplemented by system software, should be exercised by the system over the memory addresses to which a user program has access.

14. A computer or processor-based system should have the capability to effectively isolate users from each other, and from the protection control portion of the operating system. The principal hardware registers, bounds registers, and checking circuits should ensure that access to programmed memory addresses is limited to authorized programs and data.

15. Entrance to the supervisory or executive mode should be hardware controlled.

16. Certain hardware measures can be utilized in remotely accessed computer systems to provide improved means of identifying users and terminal devices. These include the use of hardware generated characters that identify the terminal to the central system, and magnetically encoded badges or cards which activate the terminal device when inserted into a reader.

## CHAPTER 9. SOFTWARE SECURITY

### A. GENERAL.

1. Software based protective controls complement and support hardware protective features designed into computer circuitry. Increasing reliance for computer system security will have to be placed upon safeguards installed within executive, utility, and applications software. Existing commercial and other standard software products offer a wide variety of security features and varying degrees of software protection. This chapter establishes general policies with respect to the security characteristics of various types of software and emphasizes some of the more desirable features which serve to enhance the security of computer systems.

2. Software categories include:

   a. General purpose software.

      (1) System software. That which controls the operations of the ADP equipment (e.g., operating systems, executive, supervisors, non-hardware input/output controllers).

      (2) Utility software. That which supports both executive and applications software (e.g., sort/merge routines, data management systems, interpreters, and converters).

      (3) Software tools. Those which are used in the development of applications software.

   b. Applications software. Functionally oriented, problem-solving software (e.g., payroll and inventory control). See Chapter 14, Sensitive Application Certification.

3. Each of the preceding categories and types of software have implications upon the overall security of the system which the user must consider in handling sensitive information. Additionally, many new types and categories of software are coming into being as both hardware and software technology advance. Many traditional control functions are being placed in programmable read-only memory (PROM), or extended through inclusion in firmware or embedded into microprocessors. These technologies offer promise for future extension of effective security measures. This chapter will focus on operating systems, data base management systems, and application software.

**B. POLICY.**

1. Software selected to process classified and sensitive information shall demonstrate positive security attributes and capabilities. Conversely, software known to possess inherent security weaknesses shall not be employed to handle sensitive information unless special managerial or procedural controls designed to minimize these weaknesses have been implemented.

2. The collective security features of applications, utility, and executive software, when used in combination, shall be complementary and serve to enhance the security effectiveness of the system.

3. Safeguards embedded in software shall be protected against compromise, subversion, or unauthorized manipulation in accordance with FIPS Pub 73.

4. The user and master modes of system operation shall be separated so that a program operating in a user mode is prevented from performing control functions. As much of the operating system as possible should run in the user mode (as opposed to the master mode), and each part of the operating system should have only as much freedom of the computer as it needs to do its job.

5. A remotely accessed computer system shall be provided with the capability to identify users and substantiate that the user is, in fact, who he claims to be.

6. Control shall be maintained at all times over the use of remote terminals. In instances where an isolated terminal which accesses sensitive information is frequently left unattended during duty hours, a "time-out" protection feature shall be provided.

7. Each properly identified system user shall be permitted by the executive or control software to access system data and resources to which he is authorized, and no more. File access authorization, security profile mechanisms, and terminal access limitations are software techniques that should be used to control or restrict user access.

8. System software shall ensure proper erasure of data resident in memory segments or on-line storage areas prior to reallocation.

9. Systems software shall include, wherever possible, the means for identifying, journaling, reporting, and assigning accountability for potential compromises or violations of system/data base integrity.

9.B.10. The use of encryption for the sole purpose of protecting sensitive information transmitted over communication circuits or processed on computer systems is authorized. However, when a comprehensive risk assessment indicates that encryption is warranted, such action shall be consistent with FIPS PUB 46.

11. Software permitting, passwords shall be used to restrict access to only those data elements (fields) that a user is authorized to access.

12. Proprietary software products will not be used for processing sensitive information unless full documentation including source code is provided to the using AIS facility.

**C. OPERATING SYSTEM SECURITY FEATURES - GENERAL.**

1. Operating system controls. The operating system will contain controls which provide the user with all information to which he is authorized access, but no more. If such controls are not feasible, output material shall be generated only within the central computer facility under the cognizance of the ADP System Security Officer (ADPSSO). As a minimum, the operating system must control:

   a. All transfers of material between memory and on-line storage devices; between the central computer facility equipment and any remote device; and between on-line storage devices.

   b. All operations associated with allocating AIS resources (e.g., memory, peripheral devices, etc.); memory protection; system interrupt; and shifting between user and master protection modes.

   c. Access to programs and utilities which are authorized to perform the various categories of maintenance (e.g., operations which effect authorized additions, deletions, or changes to data) on the operating system, including any of its elements and files. Such controls will ensure that access is limited to personnel authorized to perform particular categories of maintenance.

   d. All other programs (user programs) so that access to material is made via an access control and identification system which associates the user and the user's terminal, in the AIS with the material being accessed.

9.C.2. Test and debugging programs. User application programs and systems programs which do not violate the security or integrity of the AIS, may be debugged during system operation provided that such activity is limited to the user mode. All other system software development, experimentation, testing, and debugging will be performed on a system (or library) temporarily dedicated for these purposes.

3. Shutdown and restart. The operating system must provide for security safeguards to cover unscheduled system shutdown (aborts) and subsequent restart, as well as for scheduled system shutdown and operational start-up.

4. Other fundamental features. The following features for the operating system are also considered fundamental to the operation of an AIS. Unauthorized attempts to change, circumvent, or otherwise violate these features shall be detectable and reported within a known time by the operating system, and simultaneously cause an abort or suspension of the responsible user activity. In addition, the incident shall be recorded in the audit log and the ADP System Security Officer notified.

a. Memory/storage protection. The operating system shall protect the security of the AIS by controlling:

(1) Resource allocation (including primary and auxiliary memory).

(2) Memory access outside of assigned areas.

(3) The execution of master (supervisory) mode instructions which could adversely affect the security of the operating system.

b. Memory residue. The operating system will ensure that sensitive material or critical elements of the system do not remain as accessible residue in memory or on on-line storage devices.

c. Access controls. Access to material stored within the AIS will be controlled by the ADP System Security Officer or by automatic processes operating under separate and specific controls within the operating system. These controls are established through the use of hardware, software, and administrative safeguards.

d. Security labels. All classified material accessible by or within the AIS will be identified as to its security classification, access or dissemination

9.C.4. d. (cont'd) limitations, and appropriate downgrading/declassification instructions; and all output of the AIS will be appropriately marked. Other sensitive information may be labeled as desired.

e. Remote terminal identification. Manual and administrative procedures and/or appropriate hardware/software measures shall be established to ensure that the remote terminal from which personnel are attempting to access sensitive information has been protected and is authorized such access. Where a terminal identifier is used, for this purpose, it will be maintained in a protected file. Ideally, a dial-back system should be employed.

f. User identification. Where needed to ensure control of access and individual accountability, each user or specific group of users shall be identified to the AIS by appropriate hardware/software measures. Such identification measures must be in sufficient detail to enable the AIS to provide the user only that material which he is authorized.

g. Terminal time-out. This is an automatic software disconnection of the terminal from the computer after a pre-determined period of time has elapsed without communication between the terminal and the computer. The predetermined periods of time should decrease as the level of sensitivity of the system accessed increases. Recommended time periods are 5-15 minutes. Factors to be considered in determining the time period include:

(1) Effectiveness of other software protection features such as audit trails and audit logs.

(2) Location of the terminal.

(3) Frequency of use of the terminal.

(4) Physical and procedural controls in use.

## D. OPERATING SYSTEM SECURITY FEATURES - SPECIFIC.

1. General. Operating systems generally are considered to perform some, if not all, of the following functions: job management, task management, file management, recovery management, and surveillance management. Each of these functions, by virtue of its interactions with other parts of the system, plays an important role in the overall security of the system. In the discussion that

9.D.1. (cont'd) follows, the relevant security features associated with each operating system function will be identified.

2. Job management. Job management consists of those tasks which read the input job stream, initiate a job into execution, and terminate the job. It also allocates the system input/output (I/O) resources. In particular, it provides the user interface to the system on a job basis. The elements of job management considered are the control language, user interface, spooling, job scheduling, and job control.

a. Control language. The control language allows the user to define the work to be performed by the operating system. In particular, the control language statements indicate the beginning of a job; specifies the user's identity and password; the programs to be executed; the files to be accessed; and indicates the end-of-job control statement. For example, if there is no uniquely enforced end-of-job control statement, then one job may be able to read another user's input job stream. The user which had the second user's job stream appended to his could obtain sensitive data, including the second user's identifiers and authenticators. Finally, the semantics of this language are important to security because the system resources are allocated and subsequently accessed through it.

b. User interface. The user interface of a system is defined to be the point at which the user, the operator, or the system administrator (or their programs) are identified and interact with the system.

(1) Interactive interface. The first consideration of the SIGN-ON procedure is to establish the identity of the user and to prevent one user from masquerading as another. Passwords are commonly used to authenticate a user's identity. The password is kept on an access list maintained in the computer system and is used to establish system access. If the check fails, the user may be given additional SIGN-ON attempts. The number of attempts should be limited, three is recommended, and some compensatory procedure such as disconnecting the terminal after the limit has been reached should be initiated. Upon successful SIGN-ON, the user may initiate subsequent processing by use of control language statements. Eventually, the

9.D.2. b. (1) (cont'd) user enters a sign-off request to the job management process which invokes a job termination process for that specific user.

(2) Batch interface. In the batch mode of processing, the interface control is often exercised administratively by a control clerk, who personally recognizes the user, accepts the job, submits the job for processing, and distributes the output to the user. When there are any doubts concerning the rights of the user, the system or operations manager is normally consulted. In addition to these user interface checks by humans, the job control language may incorporate user identifiers and passwords.

(3) Operator interface. System operators are involved in several tasks which have serious security ramifications. Such functions include:

(a) System start-up and shutdown.

(b) System recovery.

(c) Operator/system communications.

The first of these tasks is critical because there must be assurance that the proper system is running. The second is important because a person attempting to penetrate a system can often take advantage of any incomplete processing to obtain data not authorized to him. The third task is critical because a malicious user must be prevented from spoofing the operator during such communications. In the case of operator/system communications, for example, messages issued by a user process and those issued by a system process must be easily distinguishable. A common oversight concerns the manner in which the system handles messages greater than the consoles capacity (i.e., the number of characters in a message is greater than the length on the typewriter line). Quite often the technique used is simply to continue the message on the next line. A potential problem exists in that a user could easily issue a message longer than a print line consisting of one blank line and followed by an appropriate system message to spoof the operator. Typically, the operator control process relays to the operator display device important

9.D.2. b. (3) (cont'd) information such as private device mount requests, system error messages, etc. In addition to responding to these, the operator can initiate and control certain system functions by inputs from the operator display device including changes in the system information, etc. In all of these activities, it is important that the operator not be able to display user programs or circumvent security mechanisms.

(4) ADP Systems Security Officer (ADPSSO) interface. The ADPSSO may utilize the system similar to other users (i.e., by means of a job). However, the ADPSSO has special privileges and authorities for accessing and modifying the user authorization profile. This profile usually defines the authorized users of the system, the sensitive files, and the user's password and access rights. The ADPSSO or the assistant ADPSSO may carry on a dialogue with the system through the use of a command language. The responsibilities of the ADPSSO in generating and controlling passwords are described elsewhere in this manual.

c. Spooling. Spooling involves the transfer of data between primary/secondary storage and local or remote I/O devices. However, for many operating systems there is little or no interpretation of the data or its security properties during this process. Classified jobs, for example, may not even be recognized as such during their spooling from a card reader. The job initiator is usually the first function to perform any security relevant checks. Consequently, the spooling function should contain the capability to determine the classification of jobs or data on input to a system. Furthermore, output containing classified information should be appropriately labeled, including a banner preceding and following all printed/punched media. In addition, printed data should be labeled with its classification.

d. Job scheduling. The primary purpose of the job scheduler is to assign system input and output resources to jobs. It must perform this function in a manner which does not involve the denial of service to users or permit unauthorized access to sensitive information. This is achieved through the use of mechanisms which prevent the simultaneous allocation of an I/O device or secondary storage space to

9.D.2. d. (cont'd) different user jobs. Mechanisms which prevent incorrect marking or naming of devices should also be employed.

e. Job control. Job control consists of those processes necessary to initiate the executive of a task, to provide for resource sychronization, and to terminate the task.

(1) Job initiator. The job initiator is responsible for the initiation of all jobs. It verifies that the user is authorized to use the system by comparing the user's identification parameters with those in the system authorization file. It also creates control information which identifies the job uniquely to the system throughout the life of the job. This information includes identification information such as user ID, account number, etc. Additionally, the job initiator selects from the input queue the next available job and allocates resources to it. This allocation depends upon the availability of system resources and the amount of resource sharing required. The main storage allocator must maintain an accurate record of available main storage space, otherwise the base or bounds registers can be incorrectly set and allocation of the same main storage to two or more users may occur. Many input/output devices such as tape drives are not shareable. Consequently, their allocation control is limited to granting or refusing access to them. Direct access devices permit sharing; consequently, a record of available mass storage space must be maintained for them. Otherwise, simultaneous allocations of the same space to different user jobs may occur.

(2) Resource synchronization. The possibility of contention can occur when a process needs to gain exclusive access to a system resource. Such conflicts can be resolved by process synchronization accomplished by means of locks. Associated with each system resource are one or more words to be used as a lock to control access to that resource. Accessing a system resource to prevent contention involves the following activities:

(a) Lock or reserve exclusive control of the resource;

9.D.2. e. (2) (b) Access the resource; and

(c) Unlock or release exclusive control of the resource.

Resource synchronization is important for two reasons. The use of locks reduces parallelism in the computer system, and hence, the lock can become a significant performance bottleneck. Secondly, if the locks are not used by the operating system prior to the updating or use of control information an undefined state may be reached which might cause information disclosure or system interdiction.

(3) Job terminator. The purpose of the job terminator is to purge jobs from the system. A job may terminate either normally or abnormally. If it terminates abnormally due to various types of abort conditions, the terminator must ensure that the resources are returned to the system and that the abnormal termination procedures do not permit breaches of security. Moreover, this process must ensure that no residual data is left behind. To ensure this, main storage and secondary storage as well as any hardware buffers must be purged of sensitive residual data (i.e., clear system programs).

3. Task management. Task management generally involves controlling the allocation of processor and main memory resources to system users. It, therefore, includes such functions as: processor allocation, main storage allocation, event synchronization, timer services, and interrupt handling.

a. Processor allocation. The processor allocator or dispatcher is a program which allocates the central processor to a particular job and permits control to be transferred to that job. It keeps tables or queues of the current status of all jobs and determines when their programs are ready for execution. Control of the processor is returned to the allocator after an interrupt is processed or upon executing certain types of instructions within a user of system program. The prime function of the processor allocator should be to fairly distribute the processor resources to all tasks and to prevent the denial of service to any one task. Poorly designed scheduling algorithms for allocating the central processing unit (CPU) to programs may result in over utilization of the CPU for some jobs while other jobs are not serviced at all.

9.D.3. b. Main storage allocation. When a job is selected for execution by the operating system, it is allocated main storage, and the storage protection hardware is properly enabled by the software. Other functions of key importance are swap control and program loading. Swap control is concerned with the systematic movement of programs and data between primary and secondary storage. There are two security considerations relevant to this function. The first is that the algorithms which support swapping should not cause thrashing and subsequent degradation of service. The second is that there must be an accurate record of which portion of main storage and secondary storage is assigned to each program. Without such a record it would be possible for several programs to be allocated the same storage resource. A program may be loaded initially (i.e., before the program begins execution, or dynamically) under program control. The program loader may do the following to load a request:

(1) Allocate main storage (if necessary) to continue the program.

(2) Allocate mass storage swapping space (if necessary) for the program.

(3) Make a check to ensure that the program being loaded is properly authorized.

c. Event synchronization. Because many potentially conflicting hardware events can occur simultaneously (e.g., the simultaneous execution of several channel programs), there must be some technique to synchronize those events. In addition to the many events that may occur concurrently in the hardware, different programs and routines can also be executing asynchronously in main storage due to multiprogramming. Without synchronization scheduling and resource allocation, conflicts would arise which would result in a denial of service. Synchronization can occur at the process level by waiting or posting a process until a specified event occurs. Such an event may be the completion of an input/output operation. If the event has not occured, the processor allocator is appropriately notified and the process is added to the queue of processes which are ineligible to use the processor. When the event has occurred, the processor allocator is notified that the process is eligible to use the processor.

9.D.3. d. Timer services. Timer services may be used to eliminate denial of service. By the use of timer services, it is possible to limit the use of the CPU. Another use of timer services is security surveillance. This function provides the time/data recording of information for audit trails and journaling.

e. Interrupt handling. The interrupt handlers, in conjunction with their corresponding hardware features, provide a mechanism for responding to attempted security violations such as attempts to execute illegal instructions, to violate storage protection, and to issue invalid input/output commands by hardware transfer of control to appropriate software routiness.

4. File management. File management controls all operations associated with input/output devices such as allocating space on direct access storage devices, storing data, naming and cataloging files, and moving data between main and secondary storage. The primary functions of concern are file access control, data access control and data management. Operating systems typically provide protection at the file level.

a. File access control. Since data has become more centralized in computer system facilities, the ability to share and protect that data becomes increasingly important. Consequently, the need for generally restricting access to files rather than permitting access is paramount. The issues are:

(1) Protection against unauthorized access to a file.

(2) Protection against access in unauthorized ways (e.g., doing a "write" operation when only a "read" operation is authorized).

(3) Protection against accidental errors in the use of the file.

The first two issues are functions that the file access control mechanism addresses, while the last one is addressed in the section on Recovery Management. The typical functions that must be performed are:

9.D.4. a. (1) Locate system data that describes the file. This involves first examining the job data base. If the file is currently in use, the job data base will contain an entry describing the file. If the file is not in use, the directory will be searched for the file.

(2) Verify user's right to access the file.

(3) Verify the user's access privileges.

(4) If the file is private, allocate a device and verify that the correct media is mounted.

A user may access any file to which he has been authorized access. Access to other directories is gained by having them appear in the user's own directory index. Directories may, therefore, be considered to be hierarchial. Whenever it is necessary to locate a file, a hierarchial search is made through the libraries known to the user. Temporary file names should also appear in a user's directory. If not, should there be a system crash, there is the possibility of having data on secondary storage with no way of accessing it. The granting of access depends upon the unique labeling of both the file and the media upon which the file resides. Such labeling permits machine checking that the requested media was properly mounted by the system operator. The actual granting of access would be determined through the use of the authorization data base. A user's request to use a file must be rejected unless the user has proper authorization to use the file and the requested privileges (e.g., write, read, etc.) are granted. A final consideration is the control over direct access space. A limit is needed on the total space that can be dynamically allocated to a user. Otherwise, a user may request and be granted all the available storage space resulting in denial of service to other users.

b. Data access control. Data access control consists of scheduling and controlling the transfer of data between main storage and secondary storage. Special facilities are required to provide data access control below the file level. Protection at the record or field level requires a data definition capability whereby the user and his access privileges can be specified.

9.D.4. c. Data management/data base management systems (DBMS). The traditional concept of the operating system as a manager of physical resources has been broadened as the concept of the integrated or corporate data base has become more widespread. Increasing use of inexpensive, massive on-line storage media, and proliferation of large integrated, on-line data bases has caused data base management to become the prime function of many contemporary operating systems. The extension of operating systems into the management of logical resources, such as is involved in the organization, accessing, security, and storage of data, has led to the development of data base management almost as a separate science. Accordingly, the subject will be treated in a separate section later in this chapter.

5. Recovery management. The need for recovery management functions is based upon the fact that there will be periods of operational discontinuity. These periods may be planned or unplanned. Planned or scheduled periods of discontinuity are needed for maintenance or configuration changes. Unscheduled periods of discontinuity may result from hardware or software failures. In any case, the protection mechanisms must be operative at all times to prevent unauthorized access or denial of service. The functions to be recovered must be explicitly defined when the system is designed so that the required information redundancy can be built into the various data and control blocks and so that historical log keeping facilities can be built into the system. This is required so that when the system crashes, the recovery function can check the viability of key data and reconstruct it, if required. Recovery management consists of hardware error control, software error control, and the start-up, restart, and shutdown functions.

a. Hardware error control. Hardware fault control routines are necessary to recover from accidental errors and prevent denial of service. They perform these functions by recovering from the hardware error if possible. In most current systems, the hardware fault control routines log all hardware errors and determine if recovery from the malfunction is possible. The functions that these routines provide are machine check handling--the recovery of errors in either the CPU or main storage; channel check handling--the recovery from lost I/O interrupts; dynamic device recovery--the recovery from a failing I/O device; and finally, alternate path retry--the operation on another channel when the hardware has

9.D.5. a. (cont'd) been appropriately configured. In each case, the malfunction is identified and logged, retried, if possible, and localized to a specific component.

b. Software error control. Software error control is needed for both application software recovery and operating system software recovery. For application software, checkpoint/restart routines are provided. The current problem with checkpoint/restart is that they record protector related data on the user checkpoint file and neglect to check it upon restart.

(1) At times, the operating system may discover system data to be incorrect or inconsistent as a result of either a hardware of software error. Provisions in current systems for responding to such conditions vary from almost no recovery actions to extensive recovery actions.

(2) For operating systems which provide system recovery, the recovery may consist of the following:

- If the problem is in a user program, then it may be terminated rather than terminating the entire operating system.

- If the problem is in a system task and it is reentrant, then the system task may be retried.

Recovery may be successful after a fresh copy of the routine has been loaded into main storage; otherwise, it might be necessary to gracefully (soft) shut down the system. These routines minimize the discontinuity of service and significantly increase the availability of the system.

c. Start-up/restart/shutdown.

(1) An operating system does not operate continuously in the same state since there are scheduled maintenance, start-up, restart, and shutdown periods and periods when the equipment is idle. However, security must be in force at all times.

(2) At system start-up, the system is loaded from the system files. This process initializes operating system files, loads routines into main storage, and defines the environment, the users,

9.D.5. c. (2) (cont'd) the resources, and the user's access privileges. Consequently, it is necessary to verify that proper system and authorization data is being loaded.

(3) Restart is necessary after a computer system failure or planned shutdown (e.g., any maintenance period, reconfiguration, or change in the authorization profile). The same considerations apply to initialization as for the start-up process. It is necessary to verify that both the operating system and authorization profile has been correctly initialized and no unauthorized changes have occurred.

(4) Shutdown is concerned with the orderly and logical termination of the operating system from an operational state to an idle state. The primary concern is the protection of resources and information during this process. As such, sufficient environmental data must be saved to permit an orderly recovery or restart.

6. Surveillance management. A surveillance function is required to assure accountability of the users of the system and to perform security damage assessment. In current systems, this function has been used to enhance recovery, to tune system operations, or to provide accounting information. Consideration should be given to applying the data ability from this function to achieve individual accountability and security damage assessment. Surveillance management consists of the security audit function and threat monitoring.

## E. DATA BASE MANAGEMENT SYSTEMS (DBMS).

1. DBMS have come into widespread use due to their ability to promote and support integrated data bases. As with other recent software advances, their design has been driven by the need to promote sharing of data. It is this feature that has created difficulties in ensuring the security and integrity of these data bases.

2. Data base management systems are intended to integrate and manage data in a nonredundant structure for processing by multiple applications. Data management systems are intended to permit access to and retrieval from existing files, usually in response to single applications, reports generation or simple information retrieval requirements. DBMS, therefore, represent a more difficult problem, technologically, in ensuring positive control over data.

**F.** **DBMS SECURITY FEATURES**. Protection of the data base is essential, as it represents a considerable asset and is often vital to mission accomplishment. Commercially available DBMS have different characteristics affecting their security suitability which should be considered when acquiring a system for handling sensitive information. These characteristics can be generally categorized as:

1. Data base access/manipulation methodology

2. Data base integrity.

3. Save/recovery/restart.

4. Audit mechanisms and utilities.

(Detailed security implications of these aspects of DBMS will be developed and published in a subsequent change to this manual).

## CHAPTER 10. COMMUNICATIONS SECURITY

**A. GENERAL.** Commandant (G-TTS) is the program manager for Communications Security (COMSEC) and will provide guidance in COMDTINST M2200.3, Telecommunications Manual. System planners and engineers designing new automated information systems should consult Commandant (G-TTS) during the early phases of their planning. Early coordination will aid in establishment of proper COMSEC requirements and ensure early inspection and technical guidance throughout the system's installation and testing. Communications security will be achieved by use of such controls as:

1. Encryption systems approved by the National Security Agency (NSA),

2. Protected wire-line distribution system (PWDS) or intrusion-resistant cables. These circuits are costly and suitable only for short-distance communication (normally within a single building or facility, which is under continuous physical/personnel security control), or

3. Approved methods of user identification/authentication.

**B. USE OF ENCRYPTION EQUIPMENT.**

1. Use of National Bureau of Standards Data Encryption Standard (DES) equipment is effective in the protection of Level II data and is authorized. Applicability and cost effectiveness of DES can be determined by a risk assessment. NSA developed encryption equipment may be recommended for certain applications using telecommunications circuits of automated systems handling sensitive unclassified information.

2. When cost factors and policy determinations prohibit the encryption of unclassified digital communications containing sensitive information, automated information systems will be provided with other operationally feasible, cost-effective protection to guard against unauthorized manipulation and disclosure of information. In some cases, a PWDS will provide the protection required in lieu of encryption equipment.

**C. ACCESS CONTROL PACKAGES.**

1. AIS which process For Official Use Only (FOUO), privacy, asset/resource, proprietary, or other sensitive information shall be safeguarded against unauthorized use by installation of software/hardware sign-on procedures.

10.C.1. (cont'd) These procedures require each authorized user to identify and authenticate himself to the system. The same principle may be further developed, if deemed necessary, by applying controls to protect individual files within a system's catalogue and/or to restrict the privileges allowed individual users and terminals.

2. Most commercially available sign-on software permits adjustment of the number of erroneous sign-on attempts before the remote terminal device is "locked out." Systems which permit many or unlimited sign-on attempts before lockout are vulnerable to automated trial and error user password generation and dialing techniques. Systems processing Level II information are allowed up to three sign-on attempts prior to automatic disconnect. For systems processing only Level III information, the ADP System Security Officer (ADPSSO) will designate the number of sign-on attempts allowed.

3. Terminal devices or users which are "locked-out" due to excessive sign-on attempts should be "unlocked" only after authorization by the designated security officer.

## CHAPTER 11. EMANATIONS SECURITY

**A. APPLICABILITY.** This chapter is applicable to those activities processing classified information.

**B. GENERAL.** Automated information systems used to process classified information have a vulnerability of compromising emanations (TEMPEST). Commandant (G-TTS) is the program manager for TEMPEST and is responsible for TEMPEST policy and procedures. COMDTINST C5510.7 series, Coast Guard Policy on Control of Compromising Emanations (U) prescribes TEMPEST control requirements for classified information processing.

## CHAPTER 12. SECURITY TEST AND EVALUATION (ST&E)

**A. GENERAL.** Security Test and Evaluation (ST&E) is a part of the accreditation process. The primary purpose for conducting an ST&E is to obtain technical information to support the DAA's decision to accredit an ADP activity or network. The ST&E consists of two interrelated phases. The first phase determines whether the necessary security controls have been installed, and the second phase determines whether the installed controls are working effectively.

The resources required for each ST&E and the level of detail required will depend upon the sensitivity of data being processed and the mode of operation. An activity processing Level I data will require an in-depth review of security controls; whereas an activity processing Level II data in a dedicated mode will require little more than reasonable assurance that adequate security is being provided to protect against unauthorized destruction, modification, or disclosure of the data, and theft, damage, or unauthorized use of the ADP equipment. The results of the risk assessment will also determine the scope and level of detail for the ST&E.

**B. POLICY.** Security Test and Evaluations are required for AIS processing Level I or Level II data. The Designated Approving Authority is responsible for ensuring the ST&E is conducted in an impartial and effective manner.

**C. PROCEDURES.** The following general procedures apply in conducting a Security Test and Evaluation.

1. Include on the ST&E team, personnel who have knowledge of the following:

   a. ADP security

   b. System hardware/software

   c. Application software

   d. Physical security

   e. Personnel and administrative security

   f. Telecommunications security

   g. Emanations security

2. Review the risk assessment for currency and accuracy and identify and analyze the nature of the threats and vulnerabilities and their respective controls. This provides a basis for the preparation of the ST&E plan.

12.C.3. Prepare the ST&E plan. This plan describes how each control will be observed or exercised to determine if it is effective. If scenarios, walk-through inspections, documentation and procedure reviews will be used, information should be put in the plan identifying the controls to be evaluated by each method.

4. Conduct the ST&E. Observe or exercise the security controls as outlined in the ST&E. Identify discrepancies and problem areas during the ST&E so recommendations can be made in the report to the DAA.

5. Document the results of the ST&E. Summarize the results of the ST&E noting discrepancies and problem areas. Include a recommendation to the DAA to accredit or not accredit (can recommend interim authority to operate if appropriate) based on the level risk and the effectiveness of the controls.

## CHAPTER 13. ACCREDITATION

**A. GENERAL.** This chapter defines accreditation requirements for automated information systems (AIS) operated by or on behalf of the Coast Guard.

1. Accreditation is the formal declaration that appropriate AIS security controls have been properly implemented for an AIS consistent with system and data protection requirements. The requirement for accreditation applies to all Coast Guard AIS. The individual steps of the accreditation process vary with the level and type of data processed by the AIS.

2. Commandant (G-T) is responsible for accrediting Level I systems other than standalone systems; accrediting authority for other systems is delegated to the Headquarter's office, area staff, district, maintenance and logistics command, Headquarter's unit and activity level depending on the sensitivity of information processed. The accrediting authority, called the Designated Approving Authority (DAA), will review the accreditation support documentation and either concur, thereby declaring that a satisfactory level of AIS security is present; or not concur, indicating that the level of risk either has not been adequately defined or has not been reduced to an acceptable level for AIS operations.

3. Automated systems not accredited may operate only if an interim authority to operate is issued by the applicable Designated Approving Authority. Interim authority to operate is not a waiver of the requirement for accreditation. The interim authority to operate permits an activity to meet its operational mission requirements while improving its AIS security posture. Guidance regarding interim authority to operate is provided in paragraph C.3.

**B. DESIGNATED APPROVING AUTHORITY.** For accreditation purposes, Coast Guard automated systems are grouped according to the sensitivity of data handled and the security mode of operation. The Designated Approving Authority (DAA) for automated information systems is as follows:

1. Level I stand-alone systems operated in accordance with the requirements of Chapter 18, Classified Information Processing: Office chiefs; area commanders; district commanders; commanding officers of regional maintenance and logistics commands; Commander, Activities Europe; and commanding officers of Headquarter's units.

2. Level I systems other than standalone: Commandant (G-T).

13.B.3. Level II systems: Office chiefs; area commanders; district commanders; commanding officers of regional maintenance and logistics commands; Commander, Activities Europe; and commanding officers of Headquarter's units.

4. Level III systems: Accreditation is not required; HOWEVER, office chiefs; area commanders; district commanders; commanding officers of regional maintenance and logistics commands; Commander, Activities Europe; and commanding officers of Headquarter's units, shall ensure appropriate physical and environmental controls, as well as contingency plans for those systems for which unplanned disruption of service would have a critical impact on mission accomplishment, are in place.

**C. ACCREDITATION PROCESS.**

1. Each Headquarter's office, area staff, district, regional maintenance and logistics command, and Headquarter's unit shall develop and maintain an AIS Security Plan or Plans which address automated systems within the command. Contents of the plan(s) are described in Chapter 14. Plans are submitted for approval to the Designated Approving Authority (DAA) responsible for accrediting the most sensitive system in the plan.

2. Risk assessments, contingency plans, and security test and evaluations must be completed prior to accreditation. The responsibilities for and the scope of these actions depends on the sensitivity of information on the system and the system type and are described in this Manual. The DAA accredits individual systems based on a review of applicable accreditation support documentation. One statement of accreditation may address more than one system, if all systems are co-located at one activity.

3. At time of accreditation, Coast Guard automated systems shall be assigned to one of three categories:

   a. AIS for which all cost effective security controls have been implemented will be accredited at the level and conditions cited in the statement of accreditation.

   b. AIS which are operating within an acceptable level of risk but with some cost effective controls not yet implemented will not be accredited, but will be allowed to operate under an interim authority to operate.

   c. AIS which are operating at an unacceptable level of risk will not be accredited and must cease operations until corrective measures have been implemented.

13.C.4. Interim authority to operate may be granted to systems not accredited based on the following:

a. Existing Systems. An interim authority to operate is granted to all CG automated information systems processing Level II data.

An interim authority to operate automated systems processing Level I data is granted to those systems which meet the requirements of Chapter 18, Classified Information Processing. Interim authority to operate all other automated systems which process Level I data will be granted on an individual basis. Office chiefs; area commanders; district commanders; commanding officers of regional maintenance and logistics commands; Commander, Activities Europe; and commanding officers of Headquarter's units processing Level I data on automated systems must advise Commandant (G-T) of the following:

(1) Command or organization name where AIS is located.

(2) Level of classified information being processed.

(3) Brief system description including physical location, hardware configuration, and application software used.

(4) Description of physical, administrative, technical, and personnel security controls being used.

(5) Name, address, and phone number of ADPSO or ADPSSO responsible for system security.

Plans for formally accrediting all existing systems must be included in the AIS Security Plan.

b. New Systems. An activity shall request an interim authority to operate a new AIS from the applicable DAA. The request shall include the activity's plan for system accreditation as provided in the AIS Security plan. The DAA shall base his decision to approve interim authority to operate on the merits of the activity's plan, including the general security posture of the activity and the reasonableness of the system accreditation schedule. Once the DAA has issued the interim authority to operate, the activity will proceed with the accreditation process as described herein.

13.C.4. c. Interim authority to operate, when approved, will be granted for a specified period of time and contingent upon certain conditions being met. The DAA shall use information provided by the AIS Security Plan and other information as appropriate to determine what specific guidance or constraints should be invoked; e.g., standard operating procedures must be documented, may not process Privacy Act data, or a request for a risk assessment must be submitted by a certain date.

5. Accreditation becomes effective when a formal, dated statement of accreditation is issued. The statement of accreditation will identify, as a minimum, the AIS being accredited and the sensitivity of data authorized. Each AIS must be re-accredited on a periodic basis not to exceed five years. Re-accreditation is required whenever a change has been made which voids the accreditation conditions. A review shall be made annually, as part of an AIS security program self-audit, to verify that accreditation is still merited. Significant changes which could impact the AIS posture include:

   a. Change in the level and type of data being processed;

   b. Major redesign of the application software;

   c. Complete revision or new release to the operating system;

   d. Major change in the hardware;

   e. Construction or modification of the AIS facility; and

   f. Security violation revealing a unprotected security vulnerability.

**D. <u>LEVEL I ACCREDITATION RESPONSIBILITIES</u>.** The following paragraphs summarize accreditation responsibilities for automated information systems which process Level I data. Numbers in parentheses indicate the order of actions to be taken. When a number is used more than once, actions referenced are performed concurrently.

1. Commanding officer of AIS activity:

   a. Provide input to office, area, district, or Headquarter's unit AIS Security Plan. (1)

   b. Prepare or assist in the preparation of a risk assessment in accordance with this Manual. (3)

13.D.1. c. Prepare a contingency plan in accordance with this Manual. (4)

d. Assist in conduct of security test and evaluation (ST&E). (6)

e. Retain copy of AIS Security Plan, accreditation support documentation, and statement of accreditation. (9)

2. Office chief; area commander; district commander; commanding officer of regional maintenance and logistics command; Commander, Activities Europe; and commanding officers of Headquarter's unit or his representative:

a. Prepare an AIS Security Plan and submit plan to applicable DAA for approval. Send copy of approved plan to Commandant (G-TDS). (1)

b. When DAA, approve AIS Security Plan. (2)

c. Prepare or assist in the preparation of a risk assessment in accordance with this Manual. (3)

d. Assist in the preparation of a contingency plan in accordance with this Manual. (4)

e. Prepare a Security Test & Evaluation (ST&E) plan. Forward plan to Commandant (G-TDS) when Commandant (G-T) is DAA. (5)

f. When Commandant (G-T) is DAA, ADPSO and command security manager: Assist Commandent (G-TDS) and (G-OIS) conduct and document results of ST&E. (6)

Otherwise, ADPSO and command security manager: Conduct and document results of ST&E. (6)

g. Prepare statement of accreditation and forward to applicable DAA recommending appropriate accreditation action. Include support documentation described in Chapter 14. (7)

h. Office chief, area commander, district commander, commanding officer of regional maintenance and logistics command, or commanding officer of Headquarter's unit: Accredit AIS as appropriate. (8)

i. Retain original of AIS Security Plan, accreditation support documentation, and statement of accreditation. (9)

13.D.3. Commandant (G-T) or his representative:

a. When DAA, approve AIS Security Plan and return Plan to office chief, area commander, district commander, commanding officer of regional maintenance and logistics command, or commanding officer of Headquarter's unit. (2)

b. When DAA, conduct and document results of ST&E. Commandant (G-OIS) will assist on a case-by-case basis. (6)

c. Commandant (G-T): When DAA, accredit AIS as appropriate. Forward original to office chief, area commander, district commander, commanding officer of regional maintenance and logistics command, or commanding officer of Headquarter's units. (8)

d. When DAA, retain copy of AIS Security Plan, accreditation support documentation, and statement of accreditation. (9)

e. Retain copy of AIS Security Plan for all other Level I systems. (9)

**E. LEVEL II ACCREDITATION RESPONSIBILITIES**. The following paragraphs summarize accreditation responsibilities for automated information systems which process Level II data. Numbers in parentheses indicate the order of actions to be taken. When a number is used more than once, actions referenced are performed concurrently.

1. Commanding officer of AIS activity:

a. Provide input to office, area, district, or Headquarter's unit AIS Security Plan. (1)

b. Prepare or assist in the preparation of a risk assessment in accordance with this Manual. (3)

c. Prepare a contingency plan in accordance with this Manual. (4)

d. Assist in conduct of ST&E. (6)

e. Retain copy of AIS Security Plan, accreditation support documentation, and statement of accreditation. (9)

13.E.2. Office chief, area commander, district commander, commanding officer of regional maintenance and logistics command, or commanding officer of Headquarter's units or his representative:

a. Prepare an AIS Security Plan and submit plan to the DAA for approval. Send copy of approved plan to Commandant (G-TDS). (1)

b. Office chief, area commander, district commander, commanding officer of regional maintenance and logistics command, or commanding officer of Headquarter's unit: Approve AIS Security Plan. (2)

c. Prepare or assist in the preparation of a risk assessment in accordance with this Manual. (3)

d. Assist in the preparation of a contingency plan in accordance with this Manual. (4)

e. Prepare a Security Test & Evaluation (ST&E) Plan. (5)

f. ADPSO and command security manager: Conduct and document results of ST&E. (6)

g. Prepare statement of accreditation and forward to applicable DAA recommending appropriate accreditation action. Include support documentation described in Chapter 14. (7)

h. Office chief, area commander, district commander, commanding officer of regional maintenance and logistics command, or commanding officer of Headquarter's unit: Accredit AIS as appropriate. (8)

i. Retain original AIS Security Plan, accreditation support documentation, and statement of accreditation. Send copy of statement of accreditation to Commandant (G-TDS). (9)

3. Commandant (G-T) or his representative:

a. Retain copy of AIS Security Plan and statement of accreditation. (9)

**F. <u>ACCREDITATION OF CONTRACTOR-OWNED AIS ACTIVITIES</u>.**

1. The commanding officer of the Coast Guard activity responsible for acquiring contractor-owned AIS support (e.g., timesharing, backup processing) shall include the contractor-owned AIS in the AIS Security Plan.

13.F.2. The Designated Approving Authority shall be determined in accordance with paragraph B.

3. Since contractor policy may preclude completion of the accreditation process for Coast Guard-owned systems (e.g., risk assessment, security test and evaluation), accreditation shall be based on documented evidence of the security posture of the contractor-owned AIS. Documentation, which may be provided by the contractor, shall demonstrate a security posture consistent with the guidelines contained in this Manual.

## CHAPTER 14. SENSITIVE APPLICATION CERTIFICATION

### A. GENERAL.

1. Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, requires federal agencies to perform periodic reviews (audits) of sensitive, computer-based applications to certify the adequacy of security controls. An application is considered sensitive if it contains or processes sensitive data (e.g. classified information, financial/accounting information, personnel data, or trade secrets) or is an integral part of operations such that its loss or subversion could result in failure of the agency to complete its mission. The reviews address the adequacy of controls that are implemented by assuring they are functioning properly and identify vulnerabilities that could result in compromise of sensitive information integrity and confidentiality or the loss of processing capability. The reviews result in the identification of those additional controls, if any, considered necessary to achieve adequate security of the application.

2. Sensitive application certification (SAC) reviews are also considered to be part of agency vulnerability assessments and internal control reviews conducted in accordance with Federal Managers Financial Integrity Act and OMB Circular A-123, Internal Control Systems. Security or other control weaknesses identified are to be included in the annual internal control assurance letter and report required by OMB A-123.

### B. POLICY.

1. Reviews and re-certifications of sensitive applications shall be performed at least every three years and must be fully documented in the official agency records.

2. After completion of the system reviews, an agency official shall certify that the system meets all applicable Federal policies, regulations, and standards, and that the results of the review demonstrate that the installed security controls are adequate for the application.

**C. PROCEDURES.**

1. Commandant (G-TDS) will maintain an inventory of Coast Guard-wide sensitive applications (e.g., JUMPS/PMIS, ARMS, MSIS) and will coordinate sensitive application certification reviews of those applications using the enclosed Sensitive Application Certification Review Methodology. Commandant (G-TDS) will provide the "technical" recommendation for system certification and the application owner or user may provide operational input (e.g., criticality of system to mission, compensating factors). The certification decision will consider both the technical and operational input.

   The certification statement, signed by the certifying official, will indicate one of three possible conditions: 1) the system is certified; i.e., it meets applicable Federal policies, regulations, and standards, 2) the system is not certified and should not continue to operate, or 3) the system is certified with qualification and may continue to operate provided additional controls are implemented within a specified time frame, otherwise certification is withdrawn.

2. Office chiefs, area commanders, district commanders, and commanding officers of Headquarter's units shall certify sensitive applications which are unique to their commands. The ADPSO shall maintain an inventory of sensitive applications for the command. Sensitive application certification (SAC) reviews shall be coordinated by the ADPSO and conducted by an organization or staff independent from the organization or staff owning the application. The Sensitive Application Certification Review Methodology shall be used.

   The certification statement, signed by the office chief, area commander, district commander, and commanding officer of Headquarter's unit, will indicate one of three possible conditions: 1) the system is certified; i.e., it meets applicable Federal policies, regulations, and standards, 2) the system is not certified and should not continue to operate, or 3) the system is certified with qualification and may continue to operate provided additional controls are implemented within a specified time frame, otherwise certification is withdrawn.

   Those commands initiating SAC reviews should contact Commandant (G-TDS) for further guidance.

14.C.3. Owners of existing sensitive applications or designers of new sensitive applications should evaluate the security posture of their applications prior to the conduct of the SAC review. The Sensitive Application Design Guide (SADG) provides general and specific design considerations for sensitive applications in the areas of access controls, processing controls, personnel, contingency planning and others. The Sensitive Application Certification Review Methodology defines the process by which applications are reviewed and provides additional design guidance. See Chapter 19, New System - Security Requirements.

## CHAPTER 15. AIS SECURITY DOCUMENTATION REQUIREMENTS

**A. GENERAL.** This chapter describes the documentation required to establish, execute, and maintain an AIS security program. AIS security program documentation provides the basis for system accreditation by formally identifying the security posture of the AIS activity and those responsible for ensuring adequate controls are implemented. The following AIS security documentation is described:

1. ADP Security Officer Assignment Letter,

2. System Security Survey,

3. AIS Security Plan,

4. Risk Assessment Documentation,

5. Security Test and Evaluation (ST&E) Plan,

6. Contingency Plan,

7. System Accreditation Documentation,

8. AIS Security Program Self-Audit Report, and

9. Sensitive Application Certification Documentation.

The scope and detail of documentation will vary between system; e.g., the level of detail of a contingency plan for a Prime 750 system is much greater than that of a standard terminal cluster. On request, Commandant (G-TDS) will provide additional guidance for the preparation of AIS security documentation.

**B. OVERVIEW OF AIS SECURITY DOCUMENTATION.**

1. ADP Security Officer Assignment Letter. This letter is the formal identification by Headquarter's office, area staff, district, Headquarter's unit of the individual who has been assigned the duties of the ADP Security Officer. When a change in assignment occurs (transfer, promotion, retirement, etc.), this information shall be submitted to Commandant (G-TDS) within 60 days identifying the new ADPSO. The notice has no prescribed format. The information required is:

   a. Name of Headquarter's office, area staff, district, or Headquarter's unit; and

   b. Name of ADP Security Officer (ADPSO), routing symbol, telephone number, mailing address, and duty hours.

15.B.2. System Security Survey. A system security survey shall be prepared and maintained for each new AIS. Copies of surveys are provided as enclosures to this Manual. Each survey requests security relevant information, including name of ADPSSO, sensitivity of data, description of controls in place, etc. and provides a summary of the security posture of the system. Information from the survey provides can be used as a source of information for subsequent risk assessments, when required. The survey is prepared by the ADPSSO and is forwarded to the Headquarter's office, area staff, district, or Headquarter's unit ADPSO. Commandant (G-TDS) will periodically request information from the surveys to report on AIS Security Program status.

3. AIS Security Plan. This plan is the mechanism for establishing, implementing, and updating a Headquarter's office's, area staff's, district's, Headquarter's unit's or activity's AIS security program. The plan contains AIS security policy and provides guidelines for AIS security procedures to be used by the activity. It documents the current AIS security environment, establishes program objectives, and outlines the plan for program implementation. A plan must include an activity accreditation schedule which identifies all AIS at the activity and outlines the method for completing the steps of the accreditation process for each AIS. Level III should be included in the plan although they do not have to be accredited.

   a. The AIS Security Plan should address the following areas:

      (1) Scope of the AIS security program,

      (2) Objectives of the AIS security program,

      (3) Commanding officer's policy statement,

      (4) AIS security organization and assignment of responsibilities, and a

      (5) Description of the current AIS security environment at the activity to include:

         (a) Hardware

         (b) Software

         (c) Physical facility and its security

         (d) Personnel

15.B.3. a. (5) (e) Communications

(f) Administrative/operating procedures

(g) Data.

(6) Activity accreditation schedule identifying the anticipated date when the following will be completed:

(a) Risk assessments

(b) Contingency plan

(c) Sensitive application certification

(d) Security test and evaluation

(e) Accreditation.

b. A single AIS Security Plan shall be prepared which addresses all automated systems within the Headquarter's office, area staff, district, or Headquarter's unit. At the ADPSO's discretion, separate plans may be prepared for each activity having an AIS or for several activities having a similar processing environment (e.g., all systems processing classified information). Chapter 13 discusses plan approval authority and plan distribution.

c. The plan should serve as a comprehensive document of security posture and plans for the commanding officer and ADPSO. The ADPSO is responsible for developing, implementing, and updating the plan.

d. After the initial plan has been developed, the plan should be revised as necessary to reflect the changing environment and requirements for AIS at the activity.

e. The plan shall be approved by the applicable Designated Approving Authority (DAA). The Headquarter's office, area staff, district, Headquarter's unit will retain original AIS Security Plans. A copy of the approved plan shall be sent to Commandant (G-TDS) and to each activity referenced in the plan.

15.B.4. Risk Assessment Documentation. Risk assessments and the accompanying documentation shall comply with the requirements contained for the applicable risk assessment methodology as described in Chapter 3. Commandant (G-TDS) can provide examples of risk assessment reports upon request.

5. Security Test and Evaluation (ST&E) Plan. The ST&E plan describes how AIS security will be tested; how security controls will be exercised to determine their effectiveness. The ST&E Plan can vary from a single page check-off list for microcomputer based systems to an extensive, multi-page, detailed procedure for minicomputers processing Level I data. Model plans can be obtained from Commandant (G-TDS).

   a. The ST&E plan should include, as appropriate:

      (1) Test team organization

      (2) Plan of action and milestones for the test

      (3) Detailed test plans and procedures

      (4) Test data.

   b. The ST&E should address all elements of the AIS security environment:

      (1) Hardware

      (2) Software

      (3) Physical facility

      (4) Personnel

      (5) Communications

      (6) Administrative/operating procedures

      (7) Data.

6. Contingency Plan. Contingency plan shall fully document procedures for disaster recovery and continuity of operations. The detail and scope of the plan depends upon the characteristics of the individual activity - the specifics of the automated system and the criticality of applications. The contingency plan should provide detailed procedures for all aspects of emergency, backup,

15.B.6. (cont'd) and recovery operations. Chapter 4 of this instruction provides requirements for a contingency plan. Activities with existing contingency plans need not reformat their plans provided they incorporate the elements identified in Chapter 4.

7. System Accreditation Documentation. System accreditation documentation consists:

a. Accreditation support documentation. Accreditation support documentation provides information to support the request for accreditation. It provides evidence that the AIS activity has effectively implemented appropriate security controls consistent with the protection requirements for the data level authorized. The documentation should include some or all of the following items of information:

(1) Name, position, and telephone number of the ADPSO, ADPSSO, or NSO who will serve as a primary point of contact for the system.

(2) Identification and location of all AIS equipment; e.g., mainframe components, on-line peripherals, peripheral processors, communications processors, encryption devices, remote terminals and devices, network interfaces, etc. (Provide charts, engineering drawings, etc.).

(3) Line diagrams showing interconnection of AIS equipment, communications lines, and protection of lines.

(4) The level of the data being processed and the type within each level (Privacy Act, propietary, personal, financial, etc.).

(5) Description of the operating system and applications software (vendor acronyms may be used for industry-wide software) for the AIS.

(6) Copy of the AIS security operating procedures and other applicable command security directives, security incident handling procedures, operating procedures, AIS product marking and distributing procedures, procedures for control of modification to operating and application software, etc.

(7) Risk assessment documentation.

15.B.7. a. (8) Contingency plan and contingency plan test results.

(9) Descriptions of all security controls.

(10) ST&E test plans

(11) ST&E test reports.

(12) Copies of previous system accreditations and interim authorities to operate.

(13) AIS Security Plan.

(14) Other documentation as required by the Designated Approving Authority.

b. Request for Accreditation. Commanding officers or ADPSO's shall submit a request for accreditation to the appropriate Designated Approving Authority (DAA) in accordance with Chapter 13. The request shall include all necessary support documentation to enable the Designated Approving Authority to make a reasoned and fair determination.

c. Statement of Accreditation. If documentation supports the request for accreditation, the DAA will issue a "Statement of Accreditation." If the DAA determines accreditation is not warranted, an "Interim Authority to Operate" may be issued. A report identifying the deficiencies in the activity's accreditation documentation will be returned with the interim authority.

8. Sensitive Application Certification Documentation. Sensitive application certification (SAC) reviews will be conducted following the guidance in Chapter 14, Sensitive Application Certification. SAC documentation, including review plans, review reports, and sensitive application certification statements, are discussed in the Sensitive Application Certification Review Methodology.

9. AIS Security Program Self-Audit Report (RCS-G-TDS-16232). Chiefs of Headquarter's offices; area and district commanders; Commander, Activities Europe; and commanding officers of Headquarter's units shall send to Commandant (G-T) by June 30 each year a summary statement of the status of their AIS Security Program. The report summarizes progress achieved toward milestones in the AIS Security Plan and includes information concerning the number and type of automated systems, sensitive applications, and the status of system accreditation and certification. Figure 15-1 provides the report content.

**AIS Security Program Self-Audit Report**

Office, area, district, or Headquarters unit name

1. Total number of automated systems within the command. (Note: A standard terminal cluster is counted as one system.)

2. Number of systems processing Level I data.

3. Number of systems processing Level II data.

4. Number of automated systems which have not been accredited. Provide as an attachment a listing of Level I and II systems not accredited. Identify systems by system name and location (OPFAC) and sensitivity level (e.g., I or II)

5. Number of sensitive applications run on automated systems within the command.

6. Number of sensitive applications which have not been certified. Provide as an attachment a listing of sensitive applications not certified. Identify systems by system name and location (OPFAC).

7. Briefly (no more than one page) describe the commands AIS Awareness and Training initiatives for the previous twelve months.

Fig. 15-1

## CHAPTER 16. MICROCOMPUTER SECURITY

**A. GENERAL.** Numerous microcomputer systems including the standard terminal are in use throughout the Coast Guard; each system has a unique set of design features which afford varying capabilities for protecting information and system resources. The objectives of security for these microcomputers are the same as those for any automated information system: confidentiality of information, integrity of information, and the availability of the systems and the information or services they support. Security controls afforded microcomputers are based on the same principles of control (physical, administrative, and technical) discussed in previous chapters. Each microcomputer installation must be evaluated individually to determine the appropriate controls to prevent threats from striking, detect that threats have struck, and recover from the damaging effects.

The following guidance is taken from NBS Special Publication 500-120, Security of Personal Computer Systems: A Management Guide. Ordering information: Superintendent of Documents, Government Printing Office, Washington DC 20402.

**B. PROTECTING THE EQUIPMENT.** The typical microcomputer system installation cannot and, generally, should not be treated like a large data center with respect to physical and environmental protection needs. Protecting the microcomputer system from theft and physical damage is not fundamentally different from protecting any other valuable equipment in the workplace (protection of information is discussed later). The only additional factors are the relatively higher value of microcomputer systems and the need for greater environmental controls. The amount of protection provided must be determined by the value of equipment and the value of the processing capability (i.e. the system criticality). In most cases absolute prevention of unauthorized physical access cannot be achieved with reasonable cost constraints, controls should be in place to ensure unauthorized access is detected. The following controls help provide a safe physical environment.

1. Theft and Damage Protection.

   a. Area Access Control. Systems should not be placed in areas which have no basic physical (area) access controls (e.g. locks on the doors and people present during working hours). Providing such simple and inexpensive controls will minimize not only the theft risk; it will also help reduce exposures to some of the more sophisticated technical problems discussed later.

16.B.1. b. Equipment Enclosures. In situations where it is not feasible to secure an entire area, the equipment should be placed in special workstation enclosures which may be closed and locked when the equipment is not in use. The enclosure can provide protection for other valuable items such as documentation, diskettes, and other equipment.

c. Equipment Lockdown Devices. Lockdown devices which secure the equipment to a table or other fixed object can be used to prevent theft. Some devices also prevent access to the system power switch which can help prevent unauthorized use of the equipment.

d. Equipment Cover Locks. It is important to prevent unauthorized access to the inside of the equipment itself to protect against component theft and provide configuration control. Many systems contain valuable expansion boards (e.g. additional memory, modems, graphics interfaces) which have significant value. Equipment lockdown devices often provide protection against access to the interior of the equipment. Devices which simply lock the equipment cover are also available for many systems.

2. Environmental Controls. Microcomputers are designed to operate in the typical office environment (i.e., without special air conditioning, electrical power control, or air contamination controls). Generally, if people are comfortable, the microcomputers will be comfortable. Nevertheless, special attention should be given to minimizing the environmental hazards to which microcomputer systems are exposed.

a. Electrical Power Quality. The typical microcomputer is sensitive to the quality of its electrical power source. In most cases, keeping the computer equipment on a power source separate from appliances or office equipment will be sufficient. Inexpensive devices are available to protect against power surges (spikes). In some cases the computer may have to be placed on an isolated power source. If local power supply quality is unusually poor (e.g. large fluctuations in voltage or frequency, voltage spikes, or frequent outages), more extensive power conditioning, battery backup, or uninterruptible power supply (UPS) systems may be required.

b. Heat and Humidity. The temperature and relative humidity found in the typical office environment are well within the operating limits of most microcomputer systems. If equipment is used in other environments, users should refer to manufacturer

16.B.2. b. (cont'd) specifications for the equipment. If portable systems are being used, avoid drastic changes in temperature or humidity. Allow sufficient time for the equipment to adjust to the new environment before operating the system.

c. Air Contaminants. The operational reliability of microcomputer systems - including equipment and magnetic media - is significantly affected by the general cleanliness of the area in which it is used. Electronic equipment naturally attract charged particles in the air. The computer should be positioned to reduce exposure to smoke, dust, and other contaminants. Air filtering or air conditioning devices help to eliminate or reduce the level of contaminants.

d. Fire and Water Damage. Microcomputer systems do not represent any more of a fire hazard than other office equipment. Readily available handheld fire extinguishers provide adequate protection in normal situations. If the value of the equipment or the information is high, additional fire detection and suppression facilities may be required. The computer should be positioned to minimize exposure to water leaks or spray (e.g. overhead piping). Inexpensive plastic covers can provide some protection against water damage and also provide protection from air contaminants.

e. Static Electricity. Static electrical charges can build up in microcomputers, especially if carpeting is used. A discharge can occur when a person touches the equipment. Such a discharge could cause damage to integrated circuit components or semiconductor memory. Anti-static sprays, carpets, or pads should be used where static electricity is a problem.

f. Radio Frequency Interference. Radio frequency (RF) interference is not generally a problem unless there are major sources of radiation nearby. In some isolated situations, RF interference from other electronic equipment can cause computer equipment to malfunction; special shielding or relocation of the computer may be required to resolve these problems.

3. Magnetic Media Protection. Particular attention should be given to the protection of magnetic media. Magnetic media is the primary repository of user's information and is most often the most vulnerable system component to damage. Protection requirements for fixed disk and flexible or "floppy" disks differ.

16.B.3. a. Fixed Disk Devices. Fixed disks (also known as hard disks) usually are self-contained sealed units that are relatively well protected from environmental contaminants. Care must be exercised when moving these units because of the danger of damage to read/write heads or other internal components.

b. Flexible Diskettes. Virtually every microcomputer system has at least one "floppy" disk drive. Flexible diskettes are the most prevalent medium for distributing software and data; the handling of diskettes is an integral part of using a microcomputer. The actual magnetic disk is contained within a protective jacket. Openings in the jacket for access by the read/write heads of the drive mechanism, are particularly vulnerable to damage. Smaller ("microfloppy") diskettes used on some systems employ a rigid plastic casing with a retractable access cover which reduces the vulnerability to rough handling and contaminants.

All users should be made aware of potential dangers and proper handling techniques for flexible disks, including:

- always store in the protective jacket
- protect from bending
- insert carefully into the drive mechanism
- maintain an acceptable temperature range (50-125 F)
- avoid direct contact with magnetic fields
- do not write directly on diskette jacket or sleeve except with felt tip pen

c. General Hazards. Exposure to ordinary contaminants (smoke, hair, doughnut crumbs, coffee, etc.) is probably the major reason for failures in magnetic media. Direct contact with magnetic devices should be avoided. Airport x-ray devices and magnets (kept six or more inches away from magnetic media) pose no danger to magnetic media. Simple wear of the magnetic media also causes failures. Backup copies should be made of all important disks; day-to-day operations should be conducted with a backup copy and not the master copy of the disk.

**C. SYSTEM AND DATA ACCESS CONTROL.** Although the physical equipment has considerable value, the purpose for having the computer is to handle information. The information itself and the ability to produce, store, and analyze it normally has considerably more value than the equipment itself. Protecting the information should be the major concern of management. Controlling access to systems and information consists of the following:

16.C. Authorization - establishing the rules which determine who may access which systems and information.

Identification - identifying users and the systems or data they are permitted to access.

Access Control - enforcing the specified authorization rules.

1. Authorization. Rules must be established by the "owners" of the resources to be controlled. Authorization rules may consist of nothing more than a statement that only members of a given group or department are to have access to a given computer or application system. On the other hand, the rules may consist of formal definitions of information classification and rules for accessing each. The type of authorization rules adopted will depend on the needs of each organization. Some type of authorization process is required.

2. Identification. Users and resources must be identified for authorization rules to be enforced. In a microcomputer environment, user identification may be implicit or explicit. In a typical situation, a user establishes "authority" to use the system simply by being able to turn it on. If such implied identification is to mean anything at all, the system must be a single user system and there must be adequate physical controls to ensure that only that user can gain access. Locked offices or equipment enclosures can provide some degree of assurance in this area. If a system is shared, then such implicit identification procedures may not be adequate.

    a. Authentication. Where shared systems are used, user identification should be authenticated in some manner. Authentication should be accomplished with some type of system "logon" process in which the user provides a non-secret identifier (e.g. name or account number) and some sort of evidence to authenticate that claim (e.g. a password). User logon (authentication) should occur whenever the system is powered up or a new user needs to use the system. User identification mechanisms for some microcomputer systems require only a single (presumably secret) code, rather than separate identifier and authentication codes. This does not provide adequate security, since it does not provide a non-secret identifier for audit and accountability purposes.

16.C.2. b. Re-authentication. Re-authentication of the user should be required whenever a different user accesses the system. On a single-user system, this is accomplished by having each user turn off the system after use; each new user must go through the standard authentication process. This procedure is difficult to enforce and is often impractical when a system must be used often. Alternative techniques include:

(1) Manual system reset - require each user to perform a "system reset" (often called a "system reboot") before leaving the computer; this will re-invoke the logon process.

(2) Automatic system reset - set up the application program to perform a system reset upon completion of processing.

(3) Automatic timeout - modify the operating system to cause a system reset after a predetermined period of system inactivity.

If user identification is established through a logon procedure, that identification can be used for subsequent access control decisions. Most single-user systems do not have mechanisms for retaining such identification for the duration of a session at the computer, so repeating the authorization process maybe necessary during the course of a user's session at the computer to control access to other resources (e.g. applications).

c. Resource (Data) Labels. Resource labeling should be used to provide a means of identifying the resources to be protected. These "resources" are usually files containing data or programs. A resource could also be the ability to perform a certain function within a given application.

(1) External Labels. Diskettes containing sensitive information should be marked with special labels or brightly colored jackets to enable personnel to identify readily those materials requiring special protection.

(2) Internal Labels. Standard file management facilities of most microcomputers provide only basic file identification capability - the file name. With some operating systems it is possible to store files in specific "directories", thus providing the ability to segregate files associated with each user or by data sensitivity.

16.C.3. Logical Access Controls. Data can be protected by preventing unauthorized persons from gaining access or by denying effective use of the information if access is gained (e.g. encrytion). Logical access controls are different for data stored on removable media than data stored on fixed media.

a. Removable media protection. Simple lock-and-key control is probably the most cost-effective protection for data resident on removable media. If diskettes containing sensitive data cannot be protected in this manner, encryption may be appropriate.

b. Non-removable media protection. If data resides on non-removable media (e.g. hard disk), preventing access to the data requires controlling access to the computer system itself (user identification) and to the data available to the user. Physical access controls (e.g. locked office space or power switch) and administrative controls (e.g. observation) must be employed to prevent unauthorized access to the system. If equipment is shared by several users and cannot be monitored at all times, hardware- and software-based security mechanisms, which can limit the type of access available to each user, may be required (e.g. menu driven user interface environment). Although certain technical skills and "unusual" actions are required, these type of "technical" access control mechanisms are vulnerable to attack if the user has an opportunity to make modifications to the hardware of software.

4. Residue Control. Data often remains on a computer system or media without knowledge to the user. Data stored in an area of disk or memory which is released for reuse generally remains on the media or in memory until overwritten. The "erase" or "delete" command usually only sets a "file deleted" indicator in the file directory and does not result in physical erasure of the data. Many programs (e.g. word processors) create and delete temporary "scratch" files which the user never sees. Purge programs, which overwrite the media should be used to ensure data "residue" cannot be read by subsequent users of the system. Sensitive disk media should not be shared among users. If a fixed disk is used, data "residue" can be controlled by: overwriting the media, encrypting sensitive files, or restricting access to one user.

16.C.5. Placement of Controls. In general, controls should be placed as "low" in the system as possible, to reduce the number of alternative paths available for circumventing them. From "lowest" to "highest" controls can be placed on the hardware, operating system, application program, and user "environment." Controls placed at lower levels tend to be stronger, but are much more difficult to design and implement. Application system and user "environment" controls are easier to design and implement, but often are easy to circumvent. The type of controls used will depend on the value of the system resources and the sensitivity of the information processed.

**D. SOFTWARE AND DATA INTEGRITY.** The formal and "official" appearance of printed materials produced by microcomputer systems can result in unwarranted confidence in the substance of those materials. Formal quality and integrity controls should be employed, particularly when applications are critical to the organization.

1. Formal Software Development. Formal controls over software development and testing should be employed for systems designed and programmed in traditional programming languages (e.g. BASIC or Pascal). Analysis and control is also applicable to generic software tools (e.g. spreadsheet and data base management system) also, particularly when they are used to build complex applications. Most generic software tools do not provide built-in routines for checking the integrity of input data.

2. Data Integrity Controls. Program controls such as data format, range checks, and redundant cross-checks can be included in applications to help ensure data integrity. Managers should require individual accountability and auditability of results, reasonable checks, and various supporting information before relying on information generated by microcomputer systems.

3. Operational Controls. Controls over the implementation of many microcomputer applications are as critical as they are for large-scale systems. In those cases, the following operational procedures should be developed.

   a. Data preparation and input handling procedures

   b. Program execution procedures

   c. Media (probably diskette of tape) procedures

   d. Output handling and distribution procedures

16.D.3. (cont'd) Various administrative controls discussed in Chapter 7 may be applicable, although personnel performing such procedures probably won't have extensive data processing or operations training.

4. Documentation. Organizations often come to rely on home-grown applications developed without formal system development procedures, including the formal documentation of data definitions or programming logic. Documentation should be prepared for all aspects of any repetitive activity which is critical to its ongoing operation.

**E. BACKUP AND CONTINGENCY PLANNING.** The problem of backup and contingency planning in a microcomputer environment is essentially the same as for other data processing activities. See Chapter 4, Contingency Planning. There are some special considerations for microcomputer users due to wide distribution of equipment and number of people involved.

1. Emergency Procedures. Any area in which people work and important information is handled should have basic emergency procedures, including:

   - alarm activation and deactivation procedures,
   - evacuation plans,
   - lockup procedures,
   - medical emergency supplies and procedures,
   - fire detection and extinguishing equipment, and
   - bomb threat procedures.

   These precautions should be put in place or updated if they don't already exist or are obsolete.

2. File Backup. Unlike most large-scale systems where backups are performed centrally by trained data processing personnel, the user is generally responsible for backup of microcomputer systems. Users of microcomputer systems should perform regular and systematic backup of files. Users should also keep backup copies of commercial software, locally maintained software, and documentation for the software.

   a. Backup approaches. For data stored on diskettes or other removable media, it is often easiest to make a backup copy of the entire volume (e.g. diskette) after use or at the end of each day. If the original volume is damaged, the backup copy is used.

      For large capacity, non-removable storage devices, where it is usually impractical to perform full volume backups on a daily basis, incremental or application-based backups should be performed. With

16.E.2. a. (cont'd) incremental backups, only those files which have been modified since the last full or incremental backup are copied to the backup medium. In many cases application-based backups are easier to implement and recover since files can be organized easier. In either case, full backups should still be performed periodically.

b. Backup media. High quality media should be used since most microcomputer systems do not have write-verification

c. Storage. Backup copies of files are normally kept to enable a user to recover data after loss due to media or hardware problems or accidents (e.g. unintentional erasure of files). These backups are normally stored in a convenient nearby location. Backup copies of critical files should be stored at a location unlikely to be jointly affected by "common" emergencies such as theft, fire, or flooding. Periodic archival copies of important, but less critical files should also be stored in an "off-site" location. If microcomputers are connected to a data communications network (e.g. local area network), backup copies can be prepared on a separate device, such as a remote host of file server, providing the physically separate storage needed for disaster recovery.

**F. MISCELLANEOUS CONSIDERATIONS.** Multi-user microcomputer systems and microcomputers used in communications environments are particularly vulnerable to accidental or intentional threats since these systems do not normally have adequate security features to assure user isolation and access control. In most local area network (LAN) systems, all nodes have the ability to read all traffic on the network. If these systems are supporting users with security requirements (e.g. users processing or storing sensitive data), appropriate administrative and physical protection must be provided.

**G. RISK ASSESSMENT REQUIREMENTS.** Risk assessment requirements for microcomputer systems are discussed in Chapter 3, Risk Management and Risk Assessment.

## CHAPTER 17. STANDARD TERMINAL SECURITY

**A. GENERAL.** Security features incorporated int he USCG standard terminal system design are limited; those security features that exist, such as password protection, are provided in software. Although passwords and various protection levels can be specified at the volume, directory and/or file level, considerable precautions must be taken to ensure the protection of sensitive applications and files. The vulnerabilities of the standard terminal and its applications (ADS, CTMail, word processing, etc.) are being reviewed by both Coast Guard and contractor personnel in order that appropriate safeguards can be identified. Also, new releases of the operating system are expected to have some security improvements. While this chapter makes no attempt to cover the gamut of possible system drawbacks and flaws which can be unique to any installation, the following interim guidance is provided pending the outcome of these studies and improvements.

**B. PHYSICAL CONTROLS.**

1. Standard terminal equipment should be located in physical areas which can be locked during off-duty time. Physical protection is particularly important for those devices which can be used to initialize or load the operating system.

2. Terminals shall be logged-out when not in use for extended periods (e.g., evenings and weekends). Terminals on systems containing sensitive files shall be logged-out when not attended (e.g., lunch time). Terminals shall not remain in the executive mode or in any utility or application (word processing, Multiplan, etc.) which can terminate in the executive mode, when unattended.

3. If standard terminals and mass storage devices are located in areas which cannot be effectively controlled physically, or information contained on the system is especially sensitive, users should power-off individual terminals and secure (or keep on their person) the key to prevent system access. It is necessary for all users on the system to power-off and remove the key in order for this approach to be effective.

4. Terminals which will be used to process sensitive information should be located to discourage over-the-shoulder browsing and should not be located where they are visible from outside the working spaces (e.g., windows, passageways).

## C. ADMINISTRATIVE CONTROLS.

1. System Usage. System administrators and system ADPSOs or ADPSSOs should know what level and type of data users have on the system.

2. Backup. System administrators should routinely (once a week is reasonable) prepare backup volumes (disk or tape) for system resident files. Users should be encouraged to backup critical files to floppies on a more frequent basis if warranted.

3. Backup storage. Backup tape files, system utility disks, and other potentially useful software should be protected in a locked cabinet or safe in a locked room. Whenever possible the storage cabinet or safe should be located in an area away from the CPU and printers. Users should lock up floppies which contain sensitive files in storage desks, cabinets, or safes. Portable floppy storage boxes, even though lockable, provide inadequate protection when left out on a desk or in plain view of passersby.

4. Passwords. Password protection is the primary security feature of the standard terminal. There are three types of passwords - volume password, directory password, and file password. Directory and file passwords have different levels of protection which may be used to meet different needs. The standard terminal documentation contains the current password levels and the protection each affords. The password scheme is an integral part of the software system and cannot be readily changed without significant impact on the operating system and individual software applications and utilities. Since the typical user, who is not a trained data processor, might easily stumble upon the volume password, the following guidelines should be followed.

   a. Passwords should be required of all users. If CTMail is in use, the system administrators should activate passwords for users, since directory and CTMail passwords must be in "sync."

   b. System administrators should educate users about passwords and ensure passwords chosen by users follow a reasonable scheme. The recommended method for the development of a password is to take a group of words or phrases familiar to the user and combine all or portions of them to form the password. On systems containing sensitive files, passwords should be no less than six (6) alphanumeric characters to minimize the risk of paswords being guessed. For example:

17.C.4. b. (cont'd) the password EVOTTUPA is derived from the phrase, "EVery Other TUesday is PAyday" and can be easily memorized. Passwords based on family member names, initials, birthdays, etc. can be easily guessed and should be avoided.

c. System administrators should have two User IDs and two unique passwords - one for system administration duties and a second User ID for daily work. The system password should be known by the system administrator and one alternate; it should be written down, sealed in an envelope, and secured.

d. System administrators should change volume passwords (using the Change Volume Name command) periodically (quarterly is reasonable).

e. System administrators should change user passwords periodically (semi-annually is reasonable).

5. Application/Utility Access. System administrators should ensure users are provided executive command sets based on need-to-know criteria. Secretarial and clerical personnel, for example, should not, under normal circumstances, require access to programming languages or system utilities. The system administrator could customize command sets for various user communities. In some cases it may be appropriate to limit a user to only one application, such as word processing. The following commands should normally be reserved for the system administrator's command set only: Dump, New Command, Debug File, Set File Protection, and Set Directory Protection.

6. Volume/Directory/File Protection.

a. System files not required by general users should be protected at the "0" level to prevent viewing/analysis by unauthorized personnel. System files such as "fileheaders.sys," "mfd.sys," and "name.users" are particularly sensitive in that directory or mail passwords are identified.

b. Initializing a volume (IVol) does not write over old information contained on the volume unless a surface test (an optional parameter) is requested. Whenever a volume which was used previously to store sensitive information is being initialized, make sure the surface test parameter is invoked to destroy all data resident on the volume.

17.C.6. c. Initializing floppies without specifying a volume password results in the writing of the password (of the current path) onto the floppy <sys>fileheaders.sys file and can easily be determined. The floppy (volume) should be password protected or the path password should be changed to a null password (two single quotes ['']) prior to initializing the floppy.

d. If there is any reason to question the confidentiality or integrity of a file, the system administrator should review system data to determine if the file has been accessed at an unusual time (e.g., off duty hours or at a time not coincident with the normal processing cycle). The "files" command can provide information regarding last date/time of file modification. the word processing "(L)ist" command can provide information regarding last date/time of file access; although, the ".user" or path of access can not be determined. System administrators should advise owners of files which are sensitive to review their own files for compromise.

e. When using the "copy" command to copy a document from one directory to another, the password associated with the source document is written to the new document in the fileheaders.sys file. Always assign a new password to the new document using "^newdocument password" after the new document name in the "file to" parameter.

7. Miscellaneous.

a. System administrators should promptly remove system access rights for any personnel no longer requiring access because of job change (within or outside the company), reduction-in-force, or if security clearance or access has been terminated for cause.

b. Logon procedures (including passwords) should not be posted on or around the standard terminal or office spaces. It is preferable that passwords not be written down at all, but in any event, they should not be disclosed unless absolutely necessary. Passwords should be changed promptly afterwards.

c. In certain modes of operation of the standard terminal, CTOS does not mask a password (i.e., replace with "#" symbols) when entered. For example, when using the Asynchronous Terminal Emulator (ATE)

17.C.7.c. (cont'd) or Multi-Terminal Entry (MTE) mode to communicate with TCC's Amdahl mainframe, the Amdahl password is not masked and remains visible on the standard terminal screen until it is scrolled off. Users should use care when entering passwords while in these modes to prevent external viewing of a password.

d. System administrators should evaluate removable hard disk (cartridge) systems for those systems used to process sensitive data. The hard disks can be locked in secure storage areas or safes as appropriate.

e. System administrators should routinely (at least once a week) run jobs to delete ".tmp" and "-Old" files maintained by the system automatically for system recovery, print spooler, etc. purposes.

f. System administrators should ensure that standard terminal equipment used to process sensitive information is "cleansed" of all sensitive data before it is returned for repair or traded within USCG or with C3. The Initialize Volume utility with the surface test parameter invoked should be used to ensure sensitive data is overwritten. If because of system malfunction, the Initialize Volume utility does not function, the hard disk should be degaussed prior to transferring possession of the equipment. Commandant (G-TDS) can provide additional guidance regarding degaussing equipment and techniques if required.

g. Floppy diskettes which contain sensitive information and need to be discarded (e.g., due to excessive bad spots/defects) should be shredded or degaussed.

**D. TECHNICAL CONTROLS.**

1. Terminal ID numbers, located in PROM in the terminal, can be identified through an operating system call. This system call (Get Terminal ID) can be used when the terminal is connected to another computer in a terminal emulator mode to identify or ensure access by authorized terminals only. This method can not be used for cluster terminal management.

2. External communications links should be disconnected during off-duty working hours unless required by the ADPSSO.

**E. RISK ASSESSMENT REQUIREMENTS.** Risk assessment requirements for standard terminals are discussed in Chapter 3, Risk Management and Risk Assessment.

## CHAPTER 18. CLASSIFIED INFORMATION PROCESSING

**A. GENERAL.** The increasing use of automated information system support in preparing classified material presents a security vulnerability which could result in the compromise of classified information. The use of automated systems which process classified information must be strictly controlled. To ensure required controls are in place, automated systems processing classified information must accredited in accordance with requirements in Chapter 13, Accreditation prior to processing.

1. Standalone systems are accredited by office chiefs; area commanders; district commanders; commanding officers of regional maintenance and logistics commands; Commander, Activities Europe; and commanding officers of Headquarter's units.

2. Systems other than standalone are accredited by Commandant (G-T). Paragraph C provides additional guidance.

**B. STANDALONE SYSTEM REQUIREMENTS.** A standalone shall consist only of a keyboard, display, CPU, printer or other output device, and mass storage device. It shall have no connection (hard or soft) to any other workstation, cluster, or system, or telecommunications system or device. The following paragraphs discuss security control requirements for standalone systems. These controls are in addition to basic control requirements discussed in other chapters in this Manual.

1. For the duration of classified processing, the system shall be kept under the constant surveillance of an authorized person, who is in a physical position to exercise direct security control over the system. Security control shall include providing appropriate safeguards to deny to unauthorized persons visual access to video and other displays containing classified information.

2. All classified documents created in the system shall be properly marked as required by COMDTINST M5500.11A, Security Manual regardless of whether they are intended to be printed or not.

18.B.3. When the system will be used by another individual during the classified processing period and the classification category or type of information or need-to-know will change, the system shall be cleared first in accordance with the procedures contained in DOD 5220.22-M, Industrial Security Manual for Safeguarding Classified Information, Chapter XIII, Security Requirements for ADP Systems.

4. Upon completion of classified processing, all removable storage media (e.g., floppy diskettes), listings, ribbons, cards, classified waste, etc. shall be dismounted or removed, collected, marked, and appropriately secured or destroyed as required by COMDTINST M5500.11A, Security Manual.

5. Queues or buffers for printers and other hardcopy output devices shall be checked and emptied to ensure classified information does not remain in the system. If they exist, other system buffers (e.g., keyboard) shall be purged prior to system shutdown to ensure classified information does not remain in them.

6. The system shall be safeguarded (stored or maintained in a secure area) as required by COMDTINST M5500.11A, Security Manual whenever classified information is left in the system (e.g., primary or secondary storage) and the system is not kept under the constant surveillance of an authorized person.

7. Operating system and application software shall be protected at the same level as the highest classification of information processed.

8. Magnetic media and equipment shall be declassified or destroyed following the procedures contained in DOD 5220.22-M, Industrial Security Manual for Safeguarding Classified Information, Chapter XIII, Security Requirements for ADP Systems.

9. Unless cleared for the level of material the automated system processes or stores, authorized maintenance personnel shall be under escort at all times to guard against viewing classified information or gaining access to passwords. If a password is inadvertently or intentionally obtained by a maintenance person, it shall be considered compromised and changed immediately.

10. TEMPEST control requirements for classified information processing are discussed in COMDTINST C5510.7 series, Coast Guard Policy on Control of Compromising Emanations (U).

**C. OTHER MODES OF OPERATION.**

1. The requirements provided above are sufficiently flexible to cover most Coast Guard classified information processing needs. If classified information processing needs cannot be met given the above requirements, notify Commandant (G-TDS). Provide the following information when known:

   a. Classification of information processed,

   b. Proposed system configuration and diagrams,

   c. Diagram of three-dimensional controlled space,

   d. Hours of operation and hours manned, and

   e. Any other information relative to the protection or vulnerability of the system and the information processed.

2. Processing classified information of different classification levels or classified and unclassified information concurrently on a multi-user system requires special controls. In such cases, classified information processing may be permitted in any one of several other modes of operation should circumstances warrant. Commandant (G-T) has the authority to make this determination. These modes include: multilevel security, controlled security, systems high security, dedicated security mode, periods processing, and least privilege.

   a. Multilevel Security Mode. Operation under an operating system (supervisor or executive) which permits various categories and types of classified information to be stored and processed concurrently in an AIS and which permits selective access to such information concurrently by personnel not cleared for the highest and most restrictive category of information in the system and users having the proper security clearances and need-to-know. The separation of personnel and information on the basis of security clearance and need-to-know is accomplished by the operating system and associated system software. Constraints may be placed on concurrent processing and storage by the Designated Approving Authority.

18.C.2. b. Controlled Security Mode. Operation of an AIS when at least some personnel (users) with access to the system have neither a security clearance nor a need-to-know for all classified material contained in the system. The separation and control of users and classified information on the basis of security clearance and security classification is accomplished by the implementation of security measures, i.e., personnel security, access controls, and the incorporation of firmware and software controls, which reduce or eliminate most system software vulnerabilities.

c. Systems High Security Mode. Operation of an AIS such that the central computer facility and all of its connected peripheral devices and remote terminals are protected in accordance with the requirements for the highest classification category and type of material contained in the system. All personnel having access to the system shall have a security clearance, but not necessarily a need-to-know, for all material contained in the system.

d. Dedicated Security Mode. Operation of an AIS such that the central computer facility, the connected peripheral devices, the communications facilities, and remote terminals are used and controlled exclusively by specific users or groups of users having a security clearance and need-to-know for the processing of classified or sensitive information.

e. Periods Processing Mode. The operation of an AIS such that various levels of security classification are processed at different times with the system being purged between periods.

f. Least Privilege Mode. The operation of an AIS such that each subject (person, process, or device) in a system be granted the most restrictive set of priviliges (or lowest clearance) needed for the performance of authorized tasks. Operation in this mode limits the damage that can result from accident, error, or unauthorized use.

**D. TRUSTED COMPUTER SYSTEM REQUIREMENTS.** A trusted computer system is a system that employs sufficient hardware and software integrity controls to allow its use for simultaneously processing a range of sensitive or classified information. The National Computer Security Center (NCSC)

18.D. (cont'd) established at the National Security Agency provides technical support to achieve that objective. NCSC developed security criteria for trusted computer systems which are provided in Trusted Computer System Evaluation Criteria (CSC-STD-001-83) and Computer Security Requirements, Guidance for Applying the Trusted Computer System Evaluation Criteria in Specific Environments (CSC-STD-003-85). The Trusted Computer System Evaluation Criteria document is commonly called "the criteria" or "the orange book" because of its distinctive orange cover. See Chapter 19, New Systems - Security Requirements for applicability of trusted criteria.

**E.** **COMMUNICATION CONTROLS**. Special controls are required when classified data is transmitted. Contact Commandant (G-TTS) for additional guidance regarding communications security requirements.

## CHAPTER 19. NEW SYSTEMS - SECURITY REQUIREMENTS

**A. GENERAL.** AIS security controls should be built in, not added on. This philosophy applies to hardware and software systems and system operation support. The methods and procedures used during system design, development, and modification can have a significant influence on the adequacy and effectiveness of controls in computer-based systems. Proper controls over these processes help make sure systems are built to meet user requirements, are developed economically, are thoroughly documented and tested, and contain appropriate internal controls and audit trails. To accomplish these goals, managers responsible for the acquisition of AIS hardware, software, and operations support shall ensure the requirements contained in this Manual are reflected in the acquisition or development of new or modified systems.

**B. GENERAL REQUIREMENTS.**

1. All acquisitions of automated information systems - hardware, software, or operation support - made by a Headquarter's office, area staff, district, or Headquarter's unit must be reviewed and approved by the ADPSO for the office or command acquiring the system to ensure applicable security requirements are incorporated. The ADPSO shall maintain acquisition documentation which identifies those security requirements invoked for the acquisition.

2. All centralized acquisitions of Coast Guard-wide automated information systems by Commandant (G-T) must be reviewed and approved by Commandant (G-TDS) to ensure applicable security requirements are incorporated. The project officer shall maintain acquisition documentation which identifies those security requirements invoked for the acquisition.

3. The Federal Information Resource Management Regulations (FIRMR), Part 201-32 - Contracting for ADP Resources, contains specific regulations regarding the implementation of AIS security requirements.

**C. HARDWARE AND SYSTEM SOFTWARE.**

1. A trusted computer system is a system that employs sufficient hardware and software integrity controls to allow its use for simultaneously processing a range of sensitive or classified information. The National Computer Security Center (NCSC) trusted computer systems security criteria are provided in Trusted Computer System

19.C.1. (cont'd) Evaluation Criteria (CSC-STD-001-83) and Computer Security Requirements, Guidance for Applying the Trusted Computer System Evaluation Criteria in Specific Environments (CSC-STD-003-85). The Trusted Computer System Evaluation Criteria document is commonly called the "the criteria" or "the orange book" because of its distinctive orange cover. Currently, a limited number of computer systems have been evaluated against trusted system criteria; those systems that have been are described in an Evaluated Products List published by NCSC.

2. Documentation for all hardware acquisitions shall include requirements for system security. Trusted criteria must be referenced in the requirements for any new, multi-user, distributed systems processing classified or sensitive information. Because of the limited population of evaluated systems, specific ratings (e.g., C2 or B1) may unnecessarily restrict competition. The criteria for security policy, accountability, assurance, and documentation features; however, can be referenced either as mandatory or evaluated option requirement in the specification on a case by case basis. Specifications for multi-user systems processing classified or sensitive information shall, as a minimum, require security features described for Class C2, Controlled Access Protection systems in National Computer Security Center's Trusted Computer System Evaluation Criteria.

3. Chapter 8, Hardware Security discusses general hardware security features. Contact Commandant (G-TDS) to determine if additional requirements are appropriate.

**D. APPLICATION SOFTWARE.**

1. Each Headquarter's office, area staff, district, Headquarter's unit shall establish a management control process to assure appropriate physical, administrative, and technical controls are incorporated into all new applications, and into significant modifications to existing applications.

   A structured methodology, such as a System Development Life Cycle (SDLC) approach, should be established to ensure appropriate security controls are incorporated in new software systems. SDLC is a commonly accepted control technique used to divide an entire system development process into distinct phases so that management can review the process at key decision points. This technique is applicable during initial system design as well as during the modification process; thus, appropriate elements of it should be used whenever changes are made to a system. SDLC is particularly

19.D.1. (cont'd) advantageous because it promotes communications between programmers and systems analysts, acceptance tester, users, internal auditors, and management personnel. Commandant (G-TDS) will establish formal SDLC policy and procedure as part of the AIS Standards Program. Until then, the following interim guidance applies.

2. AIS security requirements and specifications shall be defined and approved by the ADPSO prior to acquiring or starting formal development of applications. The results of any risk assessment of the AIS facility shall be considered in determining the appropriate controls.

3. Requirements documentation for all software development projects, either Coast Guard or contractor developed, shall include a statement of requirements for system security. Security requirements shall address the following:

   a. Data origination; including source document origination, source document authorization, source document collection and input preparation, source document error handling, and source document retention.

   b. Data input; including batch or on-line conversion and entry, validation and editing, and error handling.

   c. Data processing; including batch or on-line data processing integrity, validation and editing, and error handling.

   d. Data output; including batch or on-line output balancing and reconciliation, output distribution, and output error handling, and handling and retention of output records and accountable documents.

4. The Sensitive Application Design Guide (SADG) and Sensitive Application Certification (SAC) Review Methodology provided as enclosures to this Manual and the General Accounting Office's (GAO) Audit Guide on Evaluating Internal Controls In Computer-Based Systems are excellent references for management and staff responsible for software development. They discuss numerous internal control issues such as program testing and system acceptance, configuration management controls, and specific application controls for data origination, input, processing, and output. It is not necessary that every control be in place; the need for the various controls must be evaluated for each case.

19.D.5. Each Headquarter's office, area staff, district, Headquarter's unit shall conduct and approve design reviews and system tests, prior to placing the application into operation, to assure the proposed design meets the approved security specifications. The objective of the system tests is to verify that required physical, administrative, and technical controls are operationally adequate. The results of the design reviews and system tests shall be fully documented and maintained in official records.

6. Upon completion of the system tests, the system shall be certified to indicate the system meets all applicable Federal policies, regulations, and standards, and that the results of the tests demonstrate that installed security controls are adequate for the application.

**E. <u>OPERATIONS SUPPORT</u>.**

1. Requirements documentation for the acquisition of system operations support services shall include requirements for data center protection controls and data center management controls. Data center protection controls shall be determined based on risk assessment and shall address the following:

   a. Security and access (to the processing site, system documentation, computer programs, and output).

   b. Procedures for maintenance, storage, and access to magnetic tapes, disk packs, and other data storage media.

   c. Procedures for disaster recovery and continuity of operations.

   Data center management controls include input/output control, scheduling, malfunction reporting, and preventive maintenance procedures.

2. All contract personnel positions associated with Coast Guard AIS must be designated a sensitivity level and all contract support personnel occupying those positions are required to undergo investigations and receive appropriate clearances prior to performance of duty. See Chapter 6, Personnel Security.

3. Contract support personnel are required to adhere to Coast Guard policy and procedures regarding AIS security.

APPENDIX I
TO OMB CIRCULAR NO. A-130

# FEDERAL AGENCY RESPONSIBILITIES FOR MAINTAINING RECORDS ABOUT INDIVIDUALS

## 1. Purpose and Scope

This Appendix describes agency responsibilities for implementing the Privacy Act of 1974, 5 U.S.C. 552a as amended (hereinafter "the Act"). It applies to all agencies subject to the Act. The Appendix constitutes a revision to procedures formerly contained in OMB Circular No. A-108, now rescinded. Note that this Appendix does not rescind other guidance OMB has issued to help agencies interpret the Privacy Act's provisions, e.g., Privacy Act Guidelines (40 Federal Register 28949-28978, July 9, 1975), or Guidance for Conducting Matching Programs (47 Federal Register 21656-21658, May 19, 1982).

## 2. Definitions

a. The terms "agency," "individual," "maintain," "record," "system of records," and "routine use," as used in this Appendix, are defined in the Act (5 U.S.C. 552a (a)). The definition of "agency" in the Act differs somewhat from the definition in the Circular.

b. The term "minor change to a system of records" means a change that does not significantly change the system; that is, does not affect the character or purpose of the system and does not affect the ability of an individual to gain access to his or her record or to any information pertaining to him or her which is contained in the system; e.g., changing the title of the system manager.

## 3. Assignment of Responsibilities

a. All Federal Agencies. In addition to meeting the agency requirements contained in the Act, and the specific reporting requirements detailed in this Appendix, the head of each agency shall ensure that the following reviews are conducted as often as specified below, and be prepared to report to the Director, OMB, the results of such reviews and the corrective action taken to resolve problems uncovered. The head of each agency shall:

(1) Section (m) Contracts. Review every two years a random sample of agency contracts that provide for the maintenance of a system of records on behalf of the agency to

accomplish an agency function, in order to ensure that the wording of each contract makes the provisions of the Act apply. (5 U.S.C. 552a (m)(1))

(2) Recordkeeping Practices. Review annually agency recordkeeping and disposal policies and practices in order to assure compliance with the Act.

(3) Routine Use Disclosures. Review every three years the routine use disclosures associated with each system of records in order to ensure that the recipient's use of such records continues to be compatible with the purpose for which the disclosing agency originally collected the information. The first such review should commence immediately upon the issuance of this Appendix.

(4) Exemption of Systems of Records. Review every three years each system of records for which the agency has promulgated exemption rules pursuant to Section (j) or (k) of the Privacy Act in order to determine whether such exemption is still needed.

(5) Matching Programs. Review annually ongoing matching program in which the agency has participated during the year, either as a source or as a matching agency, in order to ensure that the requirements of the Act, the OMB Matching Guidelines, and the OMB Model Control System and Checklist have been met.

(6) Privacy Act Training. Review annually agency training practices in order to ensure that all agency personnel are familiar with the requirements of the Act, with the agency's implementing regulation, and with any special requirements that their specific jobs entail.

(7) Violations. Review annually the actions of agency personnel that have resulted either in the agency being found civilly liable under Section (g) of the Act, or an employee being found criminally liable under the provisions of Section (i) of the Act, in order to determine the extent of the problem and to find the most effective way to prevent recurrences of the problem.

(8) Systems of Records Notices. Review annually each system of records notice to ensure that it accurately describes the system. Where minor changes are needed, ensure that an amended notice is published in the Federal Register. Agencies may choose to make one annual comprehensive publication consolidating such minor changes. This requirement is distinguished from and in addition to the requirement to report to OMB and the Congress major changes to systems of records and to publish those changes in the Federal Register (see paragraph 4b of this Appendix).

b. Department of Commerce. The Secretary of Commerce shall, consistent with guidelines issued by the Director, OMB, develop and issue standards and guidelines for assuring the security of information protected by the Privacy Act in automated information systems.

c. General Services Administration. The Administrator of General Services shall, consistent with guidelines issued by the Director, OMB, issue instructions on what agencies must do in order to comply with the requirements of Section (m) of the Act when contracting for the operation of a system of records to accomplish an agency purpose.

d. Office of Personnel Management. The Director of the Office of Personnel Management shall, consistent with guidelines issued by the Director, OMB:

(1) Develop and maintain government-wide standards and procedures for civilian personnel information processing and recordkeeping directives to assure conformance with the Act.

(2) Develop and conduct training programs for agency personnel, including both the conduct of courses in various substantive areas (e.g., legal, administrative, information technology) and the development of materials that agencies can use in their own courses. The assignment of this responsibilty to OPM does not affect the responsibility of individual agency heads for developing and conducting training programs tailored to the specific needs of their own personnel.

e. National Archives and Records Administration. The Archivist of the United States shall, consistent with guidelines issued by the Director, OMB:

(1) Issue instructions on the format of the agency notices and rules required to be published under the Act.

(2) Compile and publish annually the rules promulgated under 5 U.S.C. 552a(f) and agency notices published under 5 U.S.C. 552a (e)(4) in a form available to the public.

(3) Issue procedures governing the transfer of records to Federal Records Centers for storage, processing, and servicing pursuant to 44 U.S.C. 3103. For purposes of the Act, such records are considered to be maintained by the agency that deposited them. The Archivist may disclose deposited records only according to the access rules established by the agency that deposited them.

f. Office of Management and Budget. The Director of the Office of Management and Budget will:

(1) Issue guidelines and directives to the agencies to implement the Act.

(2) Assist the agencies, at their request, in implementing their Privacy Act programs.

(3) Review the new and altered system reports agencies submit pursuant to Section (o) of the Act.

(4) Compile the annual report of the President to the Congress in accordance with Section (p) of the Act.

4. Reporting Requirements

a. Privacy Act Annual Reports. To provide the necessary information for the annual report of the President, agencies shall submit a Privacy Act Annual Report to the Director, OMB, covering their Privacy Act activities for the calendar year. The exact format and timing of the report will be established by the Director, OMB. (5 U.S.C. 552a (p)); but, agencies should, at a minimum collect, and be prepared to report the following data on a calendar year basis:

(1) Total number of active systems of records and changes to that population during the year, e.g., publications of new systems, additions and deletions of routine uses, exemptions, automation of record systems.

(2) Public comments received on agency publications and implementation activities.

(3) Number of requests from individuals for access to records about themselves in systems of records that cited the Privacy Act in support of their requests.

(4) Number granted in whole or part, denied in whole, and for which no record was found.

(5) Number of amendment requests from individuals to amend records about them in systems of records that cited the Privacy Act in support of their requests.

(6) Number granted in whole or part, denied in whole, and for which no record was found.

(7) Number of appeals of access and amendment denials and the results of such appeals.

(8) Number of instances in which individuals litigated the results of appeals of access or amendment, and the results of such litigation.

(9) Number and description of matching programs participated in either as source or matching agency.

b. New and Altered System Reports. The Act requires agencies to publish notices in the Federal Register describing new or altered systems of records, and to submit reports on these systems to the Director, OMB, and to the Congress.

(1) Altered System of Records. Minor changes to systems of records need not be reported. For example, a change in the designation of the system manager due to a reorganization would not require a report, so long as an individual's ability to gain access to his or her records is not affected. Other examples include changing applicable safeguards as a result of a risk analysis, deleting a routine use when there is no longer a need for the authorized disclosure. These examples are not intended to be all-inclusive.

The following changes are those for which a report is required:

(a) An increase or change in the number or types of individuals on whom records are maintained. For example, a decision to expand a system that originally covered only residents of public housing in major cities to cover such residents nationwide would require a report. Increases attributable to normal growth should not be reported.

(b) A change that expands the types or categories of information maintained. For example, a personnel file that has been expanded to include medical records would require a report.

(c) A change that alters the purpose for which the information is used.

(d) A change to equipment configuration (either hardware or software) that creates substantially greater access to the records in the system. For example, locating interactive terminals at regional offices for accessing a system formerly accessible only at the headquarters would require a report.

(e) The addition of an exemption (pursuant to Sections (j) or (k) of the Act). Note that, in submitting a rulemaking for an exemption as part of a report of a new or altered system, agencies will meet the reporting requirements of Executive Order No. 12291 and need not make a separate submission under that order.

When an agency makes a change to an information technology installation, telecommunication network, or any other general changes in information collection, processing, dissemination, or storage that affect multiple systems of records, it may submit a single consolidated new or altered system report, with changes to existing notices and supporting documentation included in the submission.

(2) Contents of the Report. The report for a new or altered system has three elements: a transmittal letter, a narrative statement, and supporting documentation that includes a copy of the proposed Federal Register notice. There is no prescribed format for either the letter or the narrative statement. The notice must appear in the format prescribed by the Office of the Federal Register's Document Drafting Handbook.

(a) Transmittal Letter. The transmittal letter should be signed by the senior agency official responsible for implementation of the Act within the agency and should contain the name and telephone number of the individual who can best answer questions about the system. The letter should contain the agency's assurance that the proposed system does not duplicate any existing agency systems. It should also state that a copy of the report has been distributed to the Speaker of the House and the President of the Senate as the Act requires. The letter may also include requests for waiver of the reporting time period.

(b) Narrative Statement. The narrative statement should be brief. It should make reference, as appropriate, to information in the supporting documentation rather than restating such information. The statement should:

1 Describe the purpose for which the agency is establishing the system of records.

2 Identify the authority under which the system is maintained. The agency should avoid citing housekeeping statutes, but rather cite the underlying programmatic authority for collecting, maintaining, and using the information. When the system is being operated to support an agency housekeeping program, e.g., a carpool locator, the agency may, however, cite a general housekeeping statute that authorizes the agency head to keep such records as are necessary.

3 Provide the agency's evaluation of the probable or potential effects of the proposal on the privacy of individuals.

4 Describe the relationship of the proposal, if any, to the other branches of the Federal Government and to State and local governments.

5 Provide a brief description of the steps taken by the agency to minimize the risk of unauthorized access to the system of records. A more detailed assessment of the risks and specific administrative, technical, procedural, and physical safeguards established shall be made available to OMB upon request.

6 Explain how each proposed routine use satisfies the compatibility requirement of subsection (a)(7) of the Act. For altered systems, this requirement pertains only to any newly proposed routine uses.

7 Provide OMB control numbers, expiration dates, and titles of any OMB approved information collection requirements contained in the system of records. If the request for OMB clearance of an information collection is pending, the agency may simply state the title of the collection and the date it was submitted for OMB clearance.

(c) Supporting Documentation. Attach the following to all new or altered system reports:

1 An advance copy of the new or altered system notice (consistent with the provisions of 5 U.S.C. 552a (e)(4)) that the agency proposes to publish for the new or altered system. For proposed altered systems the documentation should be in the same form as the agency proposes to publish in the public notice.

2 An advance copy of any new rules or changes to published rules (consistent with the provision of 5 U.S.C. 552a (f), (j), and (k)) that the agency proposes to issue for the new or altered system. If no changes to existing rules are required, the agency shall so state in the narrative portion of the report. Proposed changes to existing rules shall be provided in the same form as the agency proposes to publish for formal notice and comment.

(3) Timing and Distribution for Submitting New and Altered System Reports. Submit reports on new and altered systems of records not later than 60 days prior to establishment of a new system or the implementation of an altered system (5 U.S.C. 552a (o)). Submit three copies of each report to:

President of the Senate
Washington, D.C. 20510

Speaker of the House of Representatives
Washington D.C. 20515

Administrator
Office of Information and Regulatory Affairs
Office of Management and Budget
Washington, D.C. 20503

Agencies may assume that OMB concurs in Privacy Act aspects of their proposal if OMB has not commented within 60 days from the date the transmittal letter was signed. Agencies may publish system and routine use notices as well as exemption rules in the Federal Register at the same time that they send the new or

altered system report to OMB and the Congress. The 60 day period for OMB and Congressional review and the 30 day notice and comment period for routine uses and exemptions will then run concurrently.

(4) Waivers of Report Time Period. The Director, OMB, may grant a waiver of the 60 day period if the agency asks for the waiver and can demonstrate compelling reasons. Agencies may assume that OMB concurs in their request if OMB has not commented within 30 days of the date the transmittal letter was signed. When a waiver is granted, the agency is not thereby relieved of any other responsibility or liability under the Act. Note that OMB cannot waive time periods specifically established by the Act. Agencies will still have to meet the statutory notice and comment periods required for establishing a routine use or claiming an exemption.

APPENDIX II
TO OMB CIRCULAR NO. A-130

# COST ACCOUNTING, COST RECOVERY, AND INTERAGENCY SHARING OF INFORMATION TECHNOLOGY FACILITIES

1. Purpose

This Appendix establishes procedures for cost accounting, cost recovery, and interagency sharing of Federal information technology facilities. The Appendix revises procedures formerly contained in OMB Circular No. A-121, now rescinded.

2. Applicability

This Appendix applies to all information technology facilities that are operated by or on behalf of a Federal agency; provide information technology service to more than one user; operate one or more general management computers; and have obligations in excess of $3 million per year.

3. Definitions

a. The term "information technology facility" means an organizationally defined set of personnel, hardware, software, and physical facilities, a primary function of which is the operation of information technology. An information technology facility includes:

(1) The personnel who operate computers or telecommunications systems; develop or maintain software; provide user liaison and training; schedule computers, prepare and control input data; control, reproduce, and distribute output data; maintain tape and disk libraries; provide security, maintenance, and custodial services; and directly manage or provide direct administrative support to personnel engaged in these activities.

(2) The owned or leased computer and telecommunications hardware, including central processing units; associated peripheral equipment such as disk drives, tape drives, drum storage, printers, card readers, and consoles; data entry equipment; data reproduction, decollation, booking, and binding equipment; telecommunications equipment including control units, terminals, modems, and dedicated telephone and satellite links provided by the facility to enable data transfer and access to users. Hardware acquired and maintained by users of the facility is excluded.

(3) The software, including operating system software, utilities, sorts, language processors, access methods, data base processors, and other similar multi-user software required by the

facility for support of the facility and/or for general use by users of the facility. All software acquired or maintained by users of the facility is excluded.

(4) The physical facilities, including computer rooms; tape and disk libraries; stockrooms and warehouse space; office space; physical fixtures.

b. The term "full costs" means all significant expenses incurred in the operation of an information technology facility. The following elements are included:

(1) Personnel, including salaries, overtime, and fringe benefits of civilian and military personnel; training; and travel.

(2) Equipment, including depreciation for owned, capitalized equipment; equipment rental or lease; and direct expenses for noncapitalized equipment.

(3) Software, including depreciation for capitalized costs of developing, converting, or acquiring software; rental of for software; and direct expenses for noncapitalized acquisition of software.

(4) Supplies, including office supplies; data processing materials; and miscellaneous expenses.

(5) Contracted services, including technical and consulting services; equipment maintenance; data entry support; operations support; facilities management; maintenance of software; and telecommunications network services.

(6) Space occupancy, including rental and lease of buildings, general office furniture, and equipment; building maintenance; heating, air conditioning and other utilities; telephone services; power conditioning and distribution equipment and alternate power sources; and building security and custodial services.

(7) Intra-agency services, including normal agency support services that are paid by the installation.

(8) Interagency services, including services provided by other agencies and departments that are paid by the installation.

c. The term "user" means an organizational or programmatic entity that receives service from an information technology facility. A user may be either internal or external to the agency organization responsible for the facility, but normally does not report either to the manager or director of the facility or to the same immediate supervisor.

d. The term "general management computer" means a digital computer that is used for any purpose other than as a part of a process control system, space system, mobile system, or a system meeting one of the exclusions identified in the Department of Defense Authorization Act of 1982.

4. Accounting and Reimbursement for Sharing of Information Technology Facilities

a. Interagency Sharing. Agencies shall:

(1) Share their information technology facilities with users from other agencies to the maximum extent feasible;

(2) Document sharing arrangements, where the total annual reimbursement exceeds $500,000, with individual written agreements that identify:

(a) Services available for sharing;

(b) Service priority procedures and terms (e.g., quality performance standards) to be provided to each user;

(c) Prices to be charged for providing services;

(d) Reimbursement arrangements for services provided; and

(e) Arrangements for terminating the sharing agreement;

(3) Provide standard terms and conditions to users obtaining similar services insofar as possible;

(4) Include such sharing arrangements, when fully documented and part of a formal sharing program, in justifications to OMB for resource requests (see OMB Circular No. A-11, revised) and allocations. Direct funding by a shared facility should be requested only where exceptional circumstances preclude the user agency from using alternative sources.

b. Cost Accounting. Agencies shall account for the full cost of the operation of information technology facilities.

c. User Cost Distribution System. Agencies shall implement a system to distribute the full cost of providing services to all users. That system will:

(1) Be consistent with guidance provided in the Federal Information Processing Standards Publication No. 96, "Guidelines for Developing and Implementing a Charging System for Data Processing Services" (National Bureau of Standards, Department of Commerce, 1982).

(2) Price each service provided by the facility to the users of that service on an equitable basis commensurate with the amount of resources required to provide that service and the priority of service provided. The price of individual transactions may be estimated provided that they are periodically reconciled to assure that the full costs of operations are equitably distributed among all users.

(3) Directly distribute to the recipient of the services the full costs of dedicated services, including applications developed and maintained; software unique to a single application; and telecommunications equipment, including control units, terminals, modems, and dedicated telephone or satellite links provided by the facility to enable data transfer and computer access to users.

d. Cost Recovery. Consistent with statutory authority, agencies shall:

(1) Submit periodic statements to all users of agency information technology facilities specifying the costs of services provided;

(2) Recover full cost from Federal users of the facility; and

(3) Recover costs from nonfederal users of the facilities consistent with OMB Circular No. A-25.

e. Accounting for Reimbursements Received. Agencies shall:

(1) Include resource requests for the amount of planned information technology use in user budget and appropriation requests;

(2) Assure that shared facilities reduce budget and appropriation requests by the amount of planned reimbursements from users;

(3) Prepare, at the close of each fiscal year, a report that documents in the agency's official records the full past year cost of operating information technology facilities that recover more than $500,000 per year from sharing reimbursements; and

(4) Use the portion of reimbursements arising from equipment and software depreciation for the replacement of equipment and software capital assets, provided such usage is included in the agency's budget.

5. Selection of Information Technology Facilities to Support New Applications.

In selecting information technology facilities to support new applications, agencies shall establish a management control procedure for determining which facility will be used to support each significant application. This procedure shall ensure that:

(a) All alternative facilities are considered, including other Federal agency and nonfederal facilities and services;

(b) Agency rules do not require that priority be given to the use of in-house facilities; and

(c) The user of the application has primary responsibility for selecting the facility.

6. Assignment of Responsibilities

a. All Federal Agencies. The head of each agency shall:

(1) Establish policies and procedures and assign responsibilities to implement the requirements of this Appendix; and

(2) Ensure that contracts awarded for the operation of information technology facilities include provisions for compliance with the requirements of this Appendix.

b. General Services Administration. The Administrator of General Services shall:

(1) Ensure that information technology facilities designated as Federal Data Processing Centers comply with the procedures established by this Appendix;

(2) Ensure that provisions consistent with this Appendix are included in contracts for the operation of information technology facilities when acquiring services on behalf of an agency;

7. Implementation Requirements

Agencies shall implement the provisions of this Appendix effective at the beginning of fiscal year 1987.

APPENDIX III
TO OMB CIRCULAR NO. A-130

# SECURITY OF FEDERAL AUTOMATED INFORMATION SYSTEMS

## 1. Purpose

This Appendix establishes a minimum set of controls to be included in Federal automated information systems security programs; assigns responsibilities for the security of agency automated information systems; and clarifies the relationship between such agency security programs and internal control systems established in accordance with OMB Circular No. A-123, Internal Control Systems. The Appendix revises procedures formerly contained in Transmittal Memorandum No. 1 to OMB Circular No. A-71, now rescinded, and incorporates responsibilities from applicable national security directives.

## 2. Definitions

a. The term "automated information system" means an information system (defined in Section 6d of the Circular) that is automated.

b. The term "information technology installation" means one or more computer or office automation systems including related telecommunications, peripheral and storage units, central processing units, and operating and support system software. Information technology installations may range from information technology facilities such as large centralized computer centers to individual stand-alone microprocessors such as personal computers.

c. The term "sensitive data" means data that require protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. The term includes data whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary data, records about individuals requiring protection under the Privacy Act, and data not releasable under the Freedom of Information Act.

d. The term "sensitive application" means an application of information technology that requires protection because it processes sensitive data, or because of the risk and magnitude of loss or harm that could result from improper operation or deliberate manipulation of the application.

e. The term "security specifications" means a detailed description of the safeguards required to protect a sensitive application.

3. Automated Information Systems Security Programs

Agencies shall assure an adequate level of security for all agency automated information systems, whether maintained in-house or commercially. Specifically, agencies shall:

- Assure that automated information systems operate effectively and accurately;

- Assure that there are appropriate technical, personnel, administrative, environmental, and telecommunications safeguards in automated information systems; and

- Assure the continuity of operation of automated information systems that support critical agency functions.

Agencies shall implement and maintain an automated information systems security program, including the preparation of policies, standards, and procedures. This program will be consistent with government-wide policies, procedures, and standards issued by the Office of Management and Budget, the Department of Commerce, the Department of Defense, the General Services Administration, and the Office of Personnel Management. Agency programs shall incorporate additional requirements for securing national security information in accordance with appropriate national security directives. Agency programs shall, at a minimum, include four primary elements: applications security, personnel security, information technology installation security, and security awareness and training.

a. Application Security

(1) Management Control Process and Sensitivity Evaluation. Agencies shall establish a management control process to assure that appropriate administrative, physical, and technical safeguards are incorporated into all new applications, and into significant modifications to existing applications. Management officials who are the primary users of applications should evaluate the sensitivity of new or existing applications being substantially modified. For those applications considered sensitive, the management control process shall, at a minimum, include security specifications and design reviews and systems tests.

(a) Security Specifications. Agencies shall define and approve security requirements and specifications prior to acquiring or starting formal development of the applications. The results of risk analyses performed at the information technology installation where the applications will be processed should be taken into account when defining and approving security

specifications for the applications. Other vulnerabilities of the applications, such as in telecommunications links, shall also be considered in defining security requirements. The views and recommendations of the information technology user organization, the information technology installation, and the individual responsible for security at the installation shall be considered prior to the approval of security specifications for the applications.

(b) Design Reviews and System Tests. Agencies shall conduct and approve design reviews and system tests, prior to placing the application into operation, to assure the proposed design meets the approved security specifications. The objective of the system tests should be to verify that required administrative, technical, and physical safeguards are operationally adequate. The results of the design reviews and system tests shall be fully documented and maintained in the official agency records.

(c) Certification. Upon completion of the system tests, an agency official shall certify that the system meets all applicable Federal policies, regulations, and standards, and that the results of the tests demonstrate that the installed security safeguards are adequate for the application.

(2) Periodic Review and Recertification. Agencies shall conduct periodic audits or reviews of sensitive applications and recertify the adequacy of security safeguards. Audits or reviews shall evaluate the adequacy of implemented safeguards, assure they are functioning properly, identify vulnerabilities that could heighten threats to sensitive data or valuable resources, and assist with the implementation of new safeguards where required. They are intended to provide a basis for recertification of the security of the application. Recertification shall be fully documented and maintained in the official agency-records. Audits or reviews and recertifications shall be performed at least every three years. They should be considered as part of agency vulnerability assessments and internal control reviews conducted in accordance with OMB Circular No. A-123. Security or other control weaknesses identified shall be included in the annual internal control assurance letter and report required by Circular No. A-123.

(3) Contingency Plans. Agencies shall establish policies and assign responsibilities to assure that appropriate contingency plans are developed and maintained by end users of information technology applications. The intent of such plans is to assure that users can continue to perform essential functions in the event their information technology support is interrupted. Such plans should be consistent with disaster recovery and continuity of operations plans maintained by the installation at which the application is processed.

b. Personnel Security. Agencies shall establish and manage personnel security policies and procedures to assure an adequate level of security for Federal automated information systems. Such policies and procedures shall include requirements for screening all individuals participating in the design, development, operation, or maintenance of sensitive applications as well as those having access to sensitive data. The level of screening required by these policies should vary from minimal checks to full background investigations, depending upon the sensitivity of the information to be handled and the risk and magnitude of loss or harm that could be caused by the individual. These policies shall be established for both Federal and contractor personnel. Personnel security policies for Federal employees shall be consistent with policies issued by the Office of Personnel Management.

c. Information Technology Installation Security. Agencies shall assure that an appropriate level of security is maintained at all information technology installations operated by or on behalf of the Federal Government (e.g., government-owned, contractor-operated installations).

(1) Assigning Responsibility. Agencies shall assign responsibility for the security of each installation to a management official knowledgeable in information technology and security matters.

(2) Periodic Risk Analysis. Agencies shall establish and maintain a program for the conduct of periodic risk analyses at each installation to ensure that appropriate, cost effective safeguards are incorporated into existing and new installations. The objective of a risk analysis is to provide a measure of the relative vulnerabilities and threats to an installation so that security resources can be effectively distributed to minimize potential loss. Risk analyses may vary from an informal review of a microcomputer installation to a formal, fully quantified risk analysis of a large scale computer system. The results of these analyses should be documented and taken into consideration by management officials when certifying sensitive applications processed at the installation. Such analyses should also be consulted during the evaluation of general controls over the management of information technology installations conducted in accordance with OMB Circular No. A-123. A risk analysis shall be performed:

(a) Prior to the approval of design specifications for new installations;

(b) Whenever a significant change occurs to the installations (e.g., adding a local area network; changing from batch to online processing; adding dial-up capability). Agency criteria for defining significant change shall be commensurate with the sensitivity of the data processed by the installation.

(c) At periodic intervals established by the agency commensurate with the sensitivity of the data processed, but not to exceed every five years if no risk analysis has been performed during that period.

(3) Disaster and Continuity Plan. Agencies shall maintain disaster recovery and continuity of operations plans for all information technology installations. The objective of these plans should be to provide reasonable continuity of data processing support should events occur that prevent normal operations at the installation. For large installations and installations that support essential agency functions, the plans should be fully documented and operationally tested periodically, at a frequency commensurate with the risk and magnitude of loss or harm that could result from disruption of information technology support.

(4) Acquisition Specifications. Agencies shall assure that appropriate technical, administrative, physical, and personnel security requirements are included in specifications for the acquisition or operation of information technology installations, equipment, software, and related services, whether procured by the agency or by GSA. These security requirements shall be reviewed and approved by the management official responsible for security at the installation making the acquisition.

d. Security Awareness and Training Programs. Agencies shall establish a security awareness and training program to assure that agency and contractor personnel involved in the management, operation, programming, maintenance, or use of information technology are aware of their security responsibilities and know how to fulfill them. Users of information technology systems should be apprised of the vulnerabilities of such systems and trained in techniques to enhance security.

4. Assignment of Responsibilities

a. Department of Commerce. The Secretary of Commerce shall:

(1) Develop and issue standards and guidelines for assuring the security of Federal automated information systems;

(2) Establish standards, approved in accordance with applicable national security directives, for systems used to process sensitive information the loss of which could adversely affect the national security interest; and

(3) Provide technical assistance to Federal agencies in implementing Department of Commerce standards and guidelines.

b. Department of Defense. The Secretary of Defense shall:

(1) Act, in accordance with applicable national security directives, as executive agent of the government for the security of telecommunications and automated information systems that process information the loss of which could adversely affect the national security interest; and

(2) Provide technical material and assistance to Federal agencies concerning security of Federal telecommunications and automated information systems.

c. General Services Administration. The Administrator of General Services shall:

(1) Issue policies and regulations for the physical and environmental security of computer rooms in Federal buildings consistent with standards issued by the Department of Commerce and the Department of Defense.

(2) Assure that agency procurement requests for computers, software, telecommunications services, and related services include security requirements. Delegations of procurement authority to agencies by GSA under mandatory programs, dollar threshold delegations, certification programs, or other so-called blanket delegations shall include requirements for agency specification of security requirements.

(3) Assure that information technology equipment, software, computer room construction, guard or custodial services, telecommunications services, and any other related services procured by GSA meet the security requirements established and specified by the user agency and are consistent with other applicable policies and standards issued by OMB, the Department of Commerce, the Department of Defense, and the Office of Personnel Management.

(4) Issue appropriate standards for the security of Federal telecommunications systems. Standards related to systems used to communicate sensitive information, the loss of which could adversely affect the national security interest, shall be developed and issued in accordance with applicable national security directives.

d. Office of Personnel Management. The Director, Office of Personnel Management, shall maintain personnel security policies for Federal personnel associated with the design, programming, operation, maintenance, or use of Federal automated information systems. Requirements for personnel checks imposed by these policies should vary commensurate with the risk and magnitude of loss or harm that could be caused by the individual. The checks may range from merely normal reemployment screening procedures to full background investigations.

5. Reports

In their annual internal control report to the President and the Congress, required under OMB Circular No. A-123, agencies shall:

a. Describe any security or other control weaknesses identified during audits or reviews of sensitive applications or when conducting risk analyses of installations; and

b. Provide assurance that there is adequate security of agency automated information systems.

APPENDIX IV
TO OMB CIRCULAR NO. A-130

ANALYSIS OF KEY SECTIONS

1. Purpose

The purpose of this Appendix is to provide a general context and explanation for the contents of the key sections of the Circular.

2. Background

The Paperwork Reduction Act of 1980, P.L. 96-511, 94 Stat 2812, codified at Chapter 35 of Title 44 of the United States Code, establishes a broad mandate for agencies to perform their information activities in an efficient, effective, and economical manner. Section 3504 of the Act provides authority to the Director, Office of Management and Budget (OMB), to develop and implement uniform and consistent information resources management policies; oversee the development and promote the use of information management principles, standards, and guidelines; evaluate agency information management practices in order to determine their adequacy and efficiency; and determine compliance of such practices with the policies, principles, standards, and guidelines promulgated by the Director.

The Circular implements OMB authority under the Act with respect to Section 3504(b), general information policy, Section 3504(e), records management, Section 3504(f), privacy, and Section 3504(g), Federal automatic data processing and telecommunications; the Privacy Act of 1974 (5 U.S.C. 552a); Sections 111 and 206 of the Federal Property and Administrative Services Act of 1949, as amended (40 U.S.C. 759 and 487, respectively); the Budget and Accounting Act of 1921 (31 U.S.C. 1 et seq.); and Executive Order No. 12046 of March 27, 1978 and Executive Order No. 12472 of April 3, 1984, Assignment of National Security and Emergency Telecommunications Functions. The Circular complements 5 CFR 1320, Controlling Paperwork Burden on the Public, which implements other sections of the Paperwork Reduction Act dealing with controlling the reporting and recordkeeping burden placed on the public.

In addition, the Circular revises and consolidates policy and procedures in five existing OMB directives and rescinds those directives, as follows:

A-71 - Responsibilities for the Administration and Management of Automatic Data Processing Activities

Transmittal Memorandum No. 1 to Circular No. A-71 - Security of Federal Automated Information Systems

A-90 - Cooperating with State and Local Governments to Coordinate and Improve Information Systems

A-108 - Responsibilities for the Maintenance of Records about Individuals by Federal Agencies

A-121 - Cost Accounting, Cost Recovery, and Interagency Sharing of Data Processing Facilities

OMB's review of the five existing policy directives led to the conclusion that much, but not all, of their content was procedural in nature, concerned chiefly with how policies were to be carried out. OMB determined that it was important clearly to distinguish the statement of policies from the procedures for implementing those policies. For this reason, the main body of the Circular consists of basic considerations and assumptions, policies, and assignments of responsibility; the appendices to the Circular consist of procedures for implementing various policies and with analysis of key sections.

OMB developed the main body of the Circular relying upon comments on the Federal Register notice as well as other forms of Federal agency and public input, principally meetings with interested parties. For the procedural revisions, OMB relied on the assistance of interagency task groups.

The revised contents of OMB Circular No. A-71, dealing with assignments of responsibilities, are in the main body of this Circular. The contents of OMB Circular No. A-90 are rescinded entirely, with the exception of a policy statement at Section 8 (b)(17) of this Circular. Revisions of the procedural aspects of the other three policy directives--Transmittal Memorandum No. 1 to A-71, A-108, and A-121--are appendices to this Circular. Appendices I, II, and III have the same prescriptive force as the Circular; Appendix IV is an explanatory document.

On September 17, 1984, the President signed National Security Decision Directive (NSDD) No. 145, National Policy on Telecommunications and Automated Information Systems Security. The NSDD requires that the Director, OMB, review for consistency with the NSDD, and amend as appropriate, OMB Circular No. A-71, Transmittal Memorandum No. 1. The Circular and Appendix III satisfy the NSDD requirement.

3. Analysis

Section 6. Definitions

f. Access to information.

g. Dissemination of information. The Circular defines "access to information" as the function of providing to members of the public, upon their

request, the government information to which they are entitled under law. Access refers to those situations in which the government agency's role is passive; access is what the government's responsibilities are when the public comes to the government and asks for information the government has and the public is entitled to. "Dissemination," in the Circular's usage, refers to the function of distributing government information; dissemination connotes an active outreach by a government agency. Dissemination refers to those situations in which the government provides the public with information without the public having to come and ask for it.

The distinction between access and dissemination is posed in order to elaborate the responsibilities of Federal agencies for providing information to the public. Two fundamentally different situations exist: one in which the public goes to the agency to ask for information the agency holds and may or may not have disseminated; and one in which the agency chooses to take the information it holds to the public. In the first instance--access--Congress has provided specific statutory policy in the Freedom of Information Act (FOIA) and in the Privacy Act. These laws and policies concerning access to government information are explicit, well known, and now so widely accepted in practice by Federal agencies as not to require policy elaboration in this Circular. Agencies should know that, if members of the public ask for information subject to FOIA or the Privacy Act, the agencies should normally provide the information forthwith, because the public has a formal legal process for forcing the agencies to yield the information.

The relationship between access to and dissemination of information is explained below, in the discussion of 8a(8) through (12).

Section 7. Basic Considerations and Assumptions

Basic considerations and assumptions are statements that provide the underpinnings for the prescriptive policies in Section 8; they are not themselves policy statements. They are either derived from statutes or legislative history, or represent executive branch management philosophy as embodied in the Circular.

- Statements 7-a through 7-d provide the general context for management of Federal information resources.

- Statement 7-e summarizes policy found in OMB Circular No. A-76, Performance of Commercial Activities.

- Statement 7-f states a general predisposition to use up-to-date information technology to manage Federal information resources.

- Statements 7-g and 7-h pertain to the Privacy Act and the Freedom of Information Act, respectively.

- Statement 7-i pertains to the National Science and Technology Policy, Organization and Priorities Act.

- Statement 7-j pertains to the Federal Records Act.

- Statement 7-k states a relationship between Federal information policy and international information policy.

Section 8. Policies.

This section is divided into two subsections that generally correspond to the twofold definition of information resources management in Section 6-b, namely, information itself and the resources associated with information.

a. Information Management. The Paperwork Reduction Act acknowledges that information is a valuable resource and should be managed as such. Proceeding from this premise, this subsection states policies concerning the management of Federal information.

(1) and (2). Information Collection and Sharing. The Circular's basic considerations and assumptions (Section 7) establish the value of government information activities. Without question, some information created or collected by Federal agencies is so vital that the American form of government, the economy, national security, and citizens' safety and wellbeing could not continue to exist in its absence. Nothing in this Circular is intended to diminish or derogate the creation or collection of such information, nor to serve as a pretext under which a Federal agency could damage the Nation's critical needs by failing to create or collect such information. At the same time, the Paperwork Reduction Act was designed to remedy deficiencies Congress perceived in Federal information activities. In the words of the report of the House Committee on Government Operations (Report No. 96-835, p. 3):
The legislation is the result of a growing concern that the way the Government collects, uses, and disseminates information must be improved. Inefficiencies in current Federal information practices drastically reduce the effectiveness of the Government while, at the same time, drowning our citizens in a sea of forms, questionnaires, and reports.

The Act intends that the creation or collection of information be carried out within the context of efficient, effective, and economical management. When Federal agencies create or collect

information--just as when they perform any other vital functions --they consume scarce resources and such activities must be continually scrutinized in light of good management principles. The applicable principles provided in the purposes of the Act are:

- to minimize the Federal paperwork burden for individuals, small businesses, State and local governments, and other persons;

- to minimize the cost to the Federal Government of collecting, maintaining, using, and disseminating information; and

- to maximize the usefulness of information collected by the Federal Government. (44 U.S.C. 3501)

Agencies must justify the creation or collection of information in the light of their statutory functions. Policy statement 8a(9) uses the standard, "necessary for the proper performance of agency functions," taken directly from the Paperwork Reduction Act (44 U.S.C. 3504 (c)(2)). Further, the policy statement includes the requirement that the information have practical utility, as defined in the Paperwork Reduction Act (44 U.S.C. 3502 (15)) and elaborated in Controlling Paperwork Burdens on the Public (5 CFR 1320). Note that practical utility includes characteristics pertaining to the quality of information such as accuracy, adequacy, and reliability, and that, in the case of general purpose statistics or recordkeeping, practical utility means that actual uses can be demonstrated (5 CFR 1320.7 (q)). Good management and the requirement of practical utility dictate that agencies must plan from the outset for the steps in the information life cycle. The Act also stipulates that agencies must "formulate plans for tabulating the information in a manner which will enhance its usefulness to other agencies and to the public" (44 U.S.C. 3507 (a)(1)(C)). When creating or collecting information, agencies must plan how they will process and transmit the information, how they will use it, what provisions they will make for access to it, whether and how they will disseminate it, how they will store it, and finally, how the information will ultimately be disposed of. While agencies cannot at the outset achieve absolute certitude in planning for each of these processes, the requirement for information resources planning is clearly contained in the Act (44 U.S.C. 3506 (c)(1)), and the absence of adequate planning is sufficient reason not to create or collect information in the first place. Before creating or collecting new information, agencies should look first to other agencies and the private sector so as not to duplicate existing information sources or services that would satisfy their needs. The Act requires that agencies shall not conduct or sponsor information collections unless they have eliminated collections "which seek to obtain information

available from another source within the Federal Government" ((44 U.S.C. 3507 (a)(1)(A)). Each agency must also "ensure its information systems do not overlap each other or duplicate the systems of other agencies" (44 U.S.C. 3506 (c)(2)). The Act also contains provisions governing the sharing of information between agencies (44 U.S.C. 3510). Applying the policy of OMB Circular No. A-76, the Circular also requires agencies to examine the possibility of acquiring the necessary information from private sector sources.

This is not to say that information creation or collection functions should be indiscriminately turned over to other agencies or to the private sector, but rather to say that agencies have an obligation to examine other potential sources of information which may satisfy agency needs. Some information can only be created or collected by Federal agencies themselves in the exercise of the government's sovereign powers. For some information, the government can satisfy its legitimate needs only when a Federal agency is the creation or collection agent. But other information needs can be met, and in many cases are routinely met, through existing services and sources in other agencies or the private sector. In many cases there is no inherently governmental function that is served by having information collected by a Federal agency; agencies should and do consider acquiring information collection services from the private sector. The Circular emphasizes that these sources should always be looked to first in the interests of efficiency and economy.

(3) through (6). Privacy Act and Freedom of Information Act. These statements contain policy statements pertaining to the Privacy Act and incorporating the policies of OMB Circular No. A-108, which is rescinded and superseded. Agencies are to ensure that they meet the requirements of the Privacy Act regarding collection of individually identifiable information. Such information is to be maintained and protected so as to preclude intrusion into the privacy of individuals. Individuals must be accorded access and amendment rights to records, as provided in the Privacy Act. Appendix I prescribes procedures for the maintenance of records about individuals in accordance with the Privacy Act.
In addition to Privacy Act considerations, statements (3) and (4) include provisions concerning proprietary information. Agencies are to minimize their collection of proprietary information, consistent with legal requirements and operational necessity and, when such information must be collected, agencies must provide for its protection.

(7). Training. Agency personnel must receive proper training to safeguard information resources. Training is particularly important in view of the changing nature of information resources management. The development of end user computing and office automation, for example, place the

management of information and information technology in the hands of nearly all agency personnel rather than in the hands of a few employees at centralized facilities such as large computer centers. Policies and procedures for computer security, records management, protection of privacy, and other safeguards need to be incorporated into information resources management training programs.

(8) through (12). Information Dissemination.

(8) and (9). General Policy. How does the public know what information is available from Federal agencies? That is, given the distinction the Circular makes between access and dissemination, what is the relationship between the two? How does the public know what government information is accessible? The answer is: through the government's dissemination of information on what is available and how to gain to access it.

The Freedom of Information Act requires each agency to publish currently in the Federal Register, for the guidance of the public, descriptions of agency organization; where and how the public may obtain information; the general course and methods by which agency functions are determined, including all procedural requirements; rules of procedure; descriptions of forms and how to obtain them; substantive regulations; statements of general policy; and revisions to all the foregoing (5 U.S.C. 552 (a)(1)). The Privacy Act also requires publication of information concerning systems of records (see Appendix I); the Government in the Sunshine Act requires agencies to make public announcements of meetings (5 U.S.C. 552b (e)(1)). The Paperwork Reduction Act (44 U.S.C. 3507 (a)(2)) and Controlling Paperwork Burdens on the Public (5 CFR 1320) require agencies to publish notices when they submit information collection requests for OMB approval. In sum, every Federal agency has obligations to disseminate basic information to the public concerning what the agency does, how its programs operate, what the public must do to comply with laws or regulations, how to receive benefits, and how the public can use agency services. These obligations are the basic linkage between access to, and dissemination of, government information. Beyond generic requirements, specific laws affect agency dissemination of information in two ways. First, for some agencies their basic enabling legislation stipulates that information dissemination is part of their statutory mission. General purpose statistical agencies, for example, have information dissemination as part of their very reason for existence. These agencies conduct substantial information dissemination programs in order to carry out their necessary functions. In contrast, other agencies such as some regulatory agencies have basic information access, but minimal information dissemination, responsibilities; the existence of substantial information dissemination programs in such agencies would be

unusual. Second, statutes may sometimes require that agencies produce and disseminate specific information products or services. For example, the law may state that the President or head of an agency shall make reports to the Congress on given subjects; these would be legally required disseminations of information.

Beyond generic and specific statutory requirements, agencies have positive obligations to disseminate information as a necessary part of performing their functions. Each agency head must clarify the nature of these obligations for the agency's particular mission and set appropriate boundaries for dissemination functions. Before deciding to disseminate an information product or service, and periodically thereafter, an agency must be able to demonstrate that the dissemination of the product or service passes the test of either being required by law or being necessary for the proper performance of agency functions.

In conformity with the purposes of the Paperwork Reduction Act, the agency's positive obligations to disseminate information must be discharged within a responsible management framework of vinimizing costs to the Federal Government while maximizing the usefulness of the information. Efficient, effective, and economical dissemination does not translate into diminishing or limiting the flow of information from the agency to the public. To the contrary, good management of information resources should result in more useful information flowing with greater facility to the public, at less cost to the taxpayer.

Given an adequate basis for dissemination, agencies must also ask themselves whether a proposed or existing information product or service substantially duplicates similar products or services that would otherwise be available, either from another agency or from the private sector. This requirement of non-duplication, originating in the Paperwork Reduction Act, husbands scarce resources and leads to more efficient, effective, and economical information dissemination by the government.

Similarly, the fact that an agency has created or collected information is not itself a valid reason for creating a program, product, or service to disseminate the information to the public. Agencies create and collect much information, often for purely internal governmental purposes, that is not intended for dissemination, for which there is no public demand, and the dissemination of which would serve no public purpose and would not be cost-justified; e.g., compilations of routine time and attendance records for Federal employees, or publication of the thousands of pages of common carrier tariff filings by regulatory agencies. While such information may be subject to access upon request under provisions of agency statutes, the Freedom of Information Act, or the Privacy Act, the agency must demonstrate in each case the need actively to disseminate such information. Over time, changes in laws, economic conditions, or information

technology can result in changes in public demand, public purpose, (r dissemination costs; for example, an agency's shift to electronic filing of reports, perhaps carried out primarily in order to improve internal information management, might generate a public demand for electronic dissemination that could be satisfied at minimal cost to the government and also improve the performance of the agency's information access function. The decision to disseminate information, however, entails potentially significant costs, must be addressed separately from the decision to create or collect information, and must hinge upon a determination that dissemination is necessary for proper performance of agency functions.

If agencies do contemplate disseminating particular information, they should plan for its dissemination when creating or collecting the information (see 8a(1)). Planning for dissemination should proceed from the Paperwork Reduction Act premises of minimizing the cost to the government while maximizing the usefulness of information. The focus of information dissemination plans should be on elevating to a policy level decisions regarding the agency's positive obligations to disseminate information and ensuring that the agency discharges the obligations in the most efficient, effective, and economical manner.

(10) Adequate Notice. Because many government information activities are important to the government and to the public, agencies must exercise care not to act capriciously with respect to information products and services. When agencies intend to commence offering new products or services, they should provide adequate advance notice so that the public may comment as to the need for the product or service. For example, if private sector interests believe they are already offering or are about to offer the same or a similar product or service--in which event the government may potentially be entering into unfair competition--such notice will allow these interests to present their case before the product or service is launched. By the same token, if many members of the public greatly depend on a particular product or service, they should be permitted to voice their views to an agency that is contemplating termination of the product of service.

The Circular refers to "significant" information products and services. It is not the Circular's intent that agencies should follow notice and comment procedures when terminating relatively inconsequential information products and services; examples might be minor brochures or flyers, products and services that were never intended to be continuing, or for which there is now little or no public audience. Agencies should determine for themselves whether information products and services are "significant," and in some cases may wish to establish procedures and threshold criteria for making such determinations. If a product or service

is considered significant, as determined ultimately by the agency head, the agency may be well advised to follow notice and comment procedures prior to initiation or termination.

(11)(a). Reaching the Public; Avoiding Information Monopolies. When agencies have justified and made the basic decision to disseminate information, they must also satisfy conditions regarding the manner of dissemination. First, agencies must take steps to ensure that members of the public whom the agency has an obligation to reach have a reasonable ability to acquire the information. The audiences for information products and services will vary, and agencies should tailor the dissemination methods so as to place the information into the hands of those whom the agency intends to receive it.

Federal agencies are often the sole holders of certain information; hence, when they disseminate, they are sole suppliers and in a position of natural monopoly. When agencies use private sector contractors to accomplish dissemination, they must take care that they do not permit contractors to exercise monopolistic controls in ways that defeat the agencies' information dissemination obligations, for example, by setting unreasonably high prices. In some cases agencies may need to formulate contractual terms with a sole supplier contractor so that the contractor functions as a mere intermediary for the agency in dealing with end users in the public.

(11)(b). Reliance on the Private Sector. In disseminating information--as with other activities--agencies must act in the most cost effective manner, which includes maximum feasible reliance on the private sector. This is merely an application to agency information dissemination programs of the policy stated in OMB Circular No. A-76, Performance of Commercial Activities, and summarized in Section 7f of this Circular. It is "the general policy of the government to rely on commercial sources to supply the products and services the government needs," including products and services the government needs in order to disseminate information to the public. For example, before an agency establishes a service for electronic dissemination of government information via an online computer system, the agency should compare the cost of contracting for operation of the service versus in-house performance and determine whether in-house performance is less costly both for the government and for the public who will receive the service.

Policies contained in OMB Circular No. A-76 are applicable to information dissemination, including the policy that inherently governmental functions should be performed by government employees. The general policy of reliance on the private sector is balanced by the "inherent governmental function" policy, and the Circular in no way intends to abrogate the latter. Where agencies determine that information dissemination activities are inherently governmental, the agencies themselves should carry out the activities.

(11)(c). User Charges. The Federal Government is the sole possessor and supplier of certain types of information, which is frequently of substantial commercial value. Dissemination of such information, or its dissemination in a specific form or medium, may represent a government service from which identifiable recipients derive special benefits, in which case they may be subject to OMB Circular No. A-25, User Charges. For example, where the information is already substantially available in printed form, agencies may consider dissemination in electronic form to be a service of special benefit, the costs of which should be recovered through user charges. Many agencies do not have consistent, agency-wide policies and procedures for setting user charges for information products and services with a view to cost recovery. Agencies must establish user charges for the costs of information dissemination, and recover such costs, where appropriate. Whether user charges are appropriate depends, in principle, on whether identifiable recipients will receive special benefits from information products and services.

The requirement to establish user charges is not, however, intended to make the ability to pay the sole criterion for determining whether the public receives government information. Agencies must balance the requirement to establish user charges and the level of fees charged against other policies, specifically, the proper performance of agency functions and the need to ensure that information products and services reach the public for whom they are intended (see Section 8a (11)(a)). If an agency has a positive obligation to place a given product or service in the hands of certain specific groups or members of the public and also determines that user charges will constitute a significant barrier to discharging this obligation, the agency may have grounds for reducing or eliminating its user charges for the product or service, or for exempting some recipients from the charge.

(12). Periodic Review and Depository Libraries. Agencies must also establish procedures for periodically reviewing their information dissemination programs. Agency information dissemination plans must ask whether the agency should disseminate a given information product or service at all; if the agency is already disseminating the product or service, reviews should ask whether the agency should continue to do so; or whether the manner or medium of dissemination is the most efficient, effective, and economical.

In addition, agencies must establish procedures to ensure compliance with 44 U.S.C. 1902, which requires that government publications (defined in 44 U.S.C. 1901 and repeated in Section 6k of the Circular) be made available to the Federal depository libraries through the Government Printing Office. The depository libraries provide a kind of information "safety net" to the public, an existing institutional mechanism that guarantees a minimum level of availability of government information to all

members of the public. Providing publications to the depository library program complies with the law and costs executive agencies virtually nothing.

b. Information Systems and Information Technology Management. This subsection states policies concerning the planning, acquisition, operation, and management of Federal information systems and technology. The Federal information systems and technology budget, which was $14 billion in FY 1985, is projected to increase at a rate faster than that of the overall Federal budget. With outlays at these levels and agencies becoming increasingly dependent upon information technology to accomplish their missions, it is essential that planning processes be applied to the acquisition and application of information technology.

(1). Planning. The Paperwork Reduction Act mandates a stronger central role in information resources planning. Specifically, the Act requires that OMB: (1) publish a five-year government-wide automatic data processing and telecommunications plan; (2) review and coordinate agency proposals for the acquisition and use of information technology; and (3) promote the use of the technology to improve governmental efficiency and effectiveness. In order to meet these objectives, it is necessary to initiate a government-wide process for developing and institutionalizing information technology planning that is based in agency programs and missions. The planning must also be tied to the budget so that budgetary decisions derive from plans, and conversely, so that budgetary constraints are reflected in the plans. The process must further ensure that sufficient information is available to the central agencies to enable them to monitor compliance with Federal policies and identify major issues, including cross-cutting issues where more active centralized planning and management may be appropriate. Hence, agencies must institute information planning processes tied to both the conduct of programs and the preparation of the agency's budget.

(2) and (3). Management Controls and Accountability. Basic management controls for agency information systems are fundamental to sound information resources management. These controls should ensure the documentation and periodic review of major information systems, as well as periodic cost-benefit evaluation of overall information resources management in light of agency missions. In order to provide greater incentive for management efficiencies, accountability for information systems should be vested in the officials responsible for operating the programs that the systems support.

Program managers depend upon information systems to carry out their programs, and yet frequently they do not have direct control over the technical and operational support for those systems. Program managers often depend upon agency computer centers or contracted service organizations, the heads of which

may not be directly accountable to the program managers in a formal organizational sense. Program managers are nonetheless responsible for conducting their programs and, to the extent successful conduct of the programs entails support from information systems, program managers must be held accountable for acquiring that support. The responsibilities of program managers are therefore presumed to include securing information systems support as needed, and planning for contingencies. Technical support organizations have a concomitant responsibility to meet their commitments, contractual or otherwise, to their program clients, but the program official has the ultimate responsibility for delivering a program's product or service.

(4) and (5). Sharing Information Processing Capacity. OMB Circular No. A-121, which is rescinded and superseded, required only that the holder of excess automatic data processing capacity share such capacity. Because the holder of excess capacity has little incentive to seek opportunities for sharing, however, the new policy requires both that the holder share capacity and that the agency seeking information processing capacity fulfill its needs from other agencies or the private sector, whenever possible, before acquiring the new capacity itself. The policy establishes an order of preference in meeting needs--look first to existing sources before acquiring new capacity--but is not intended to assert blindly that sharing or commercial sources are the sole considerations. Agencies must also consider whether existing sources are more cost effective and whether they in fact will meet agency specific needs. Procedural aspects of these policy statements are found in Appendix II.

(6) and (7). Life Cycle Costing; and Avoiding Duplication. Agencies frequently develop information technology incrementally, through a series of interim upgrades, without regard for longer term considerations such as the information systems' life cycle. As part of their planning, agencies need to consider the full information system life cycle when determining the cost of information technology. While competitive procurement is generally to be valued, its costs should be taken into account, including the cost to program effectiveness of unnecessarily lengthy procurement processes. Other conditions, such as the need for compatibility, may also be legitimate limitations on the competitive process. Similarly, agency planning should ensure that information systems are not unnecessarily duplicative of systems available elsewhere in government or from the private sector.

(8). Software Management. The prevailing agency practice of developing customized computer software is a source of inefficiency, as the General Accounting Office and others have noted. While some agency applications can only be satisfied with customized software, the tendency to prefer custom development is excessively costly in terms of initial development, continued maintenance, and eventual conversion to new technology, because

it requires the agency to bear the full cost of developing and maintaining the software it uses. While recognizing that off-the-shelf software has pitfalls, such as uncertainty of continued maintenance, managers are generally to prefer acquiring generic, off-the-shelf software available from the private sector instead of developing their own.

(9). Necessary Compatibility. Agencies often acquire technology that is incapable of communicating with other systems with which the agencies need to communicate. Compatibility among information systems has consequently emerged as a significant information resources management problem. Agencies must acquire or develop information systems in a manner that enhances necessary compatibility. The qualifier "necessary" is used because compatibility is not an unrestricted goal; information systems need to be compatible with other systems only to the extent that they must communicate with those systems.

(10) through (13). Security. Security of information systems means both the protection of information while it is within the systems and also the assurance that the systems do exactly what they are supposed to do and nothing more. Information system security entails management controls to ensure the integrity of operations including such matters as proper access to the information in the systems and proper handling of input and output. In this sense, security of information systems is first and foremost a management issue and only secondly a technical problem of computer security.

The recent introduction of smaller and more powerful computer systems and new communications technology and transmission media, together with the greater involvement of end users in managing information resources, have increased the potential vulnerability of Federal information systems and hence the level of management concern. Protecting personal, proprietary, and other sensitive data from unauthorized access or misuse; detecting and preventing computer related fraud and abuse; and assuring continuity of operations of major information systems in the event of emergency related disruptions are increasingly serious policy issues. Policy previously found in Transmittal Memorandum No. 1 to OMB Circular No. A-71 is here revised; procedural aspects of the policy are in Appendix III to the Circular.

The General Accounting Office reported in its review of the first-year implementation of the Federal Managers Financial Integrity Act (FIA) that internal controls in automatic data processing systems received inadequate coverage in FIA evaluations. GAO noted that some agencies were uncertain of the relationship between (a) OMB Circular No. A-71, Transmittal Memorandum No. 1, Security of Federal Automated Information Systems, and (b) OMB Circular No. A-123, Internal Control Systems. The relationship between security of automated information systems and agency internal control reports is now stated clearly in Appendix III.

Appendix III provides a minimal set of requirements for the security of all Federal automated information systems. The Appendix also requires agencies to incorporate additional requirements for the security of information classified for national security purposes, in accordance with appropriate national security directives.

(14). Standards. The National Bureau of Standards, Department of Commerce, develops and issues Federal Information Processing Standards. The National Communications System develops and the General Services Administration issues Federal Telecommunications Standards. Some standards are mandatory for Federal agencies, while others are voluntary. Agencies may waive the use of Federal standards under certain conditions and pursuant to certain procedures, which vary depending upon the individual standard. In general, OMB strongly recommends use of these standards government-wide. Such standards can contribute to overall government economy and efficiency by increasing compatibility in computer and telecommunications networks, improving the transportability of software, and enabling computer systems to be developed using components of different manufacturers. These advantages can result in reduced procurement costs for equipment and services, improved competition, and better utilization of staff training and skills. While government-wide standards can result in management efficiencies, agencies should be mindful that standards can also have the untoward effects of regulations, as noted in OMB Circular No. A-119. Agencies should continuously assess relative costs and benefits of standards and their effects upon the agency's accomplishment of its mission. Note also that national security directives prescribe standards for computer security.

(15). Avoiding Information Technology Monopolies. Many agencies operate one or more central information technology facilities to support agency programs. In these agencies, program managers are often required to use the central facilities. The manager of such a monopoly facility has a lesser incentive to control costs, since he or she has a captive clientele. The program manager has little leverage to ensure that information processing resources are efficiently allocated since he or she cannot seek, or can seek only with great difficulty, alternative sources of supply. When users are dependent on effective technology support to perform their functions, control over selection of facility is essential and consistent with holding users responsible for producing their government information products. To provide incentives conducive to more businesslike procedures in information technology facilities, agencies should avoid monopolistic information processing arrangements and should enter into them only if their cost effectiveness is clear and they are subject to periodic review. Appendix II specifies certain procedures with respect to this policy.

(16) Cost Recovery. This policy constitutes a revision to policy stated in OMB Circular No. A-121. Whereas Circular No. A-121 required only that costs for automatic data processing facilities be allocated to users, agencies must now recover the costs of information technology facilities from government users. Viable management of a large information technology facility requires that managers know the amount of resources devoted to each user when providing services. Furthermore, effective management of the use of information technology requires that the user have responsibility for and control over the resources consumed by use of the facility. Experience with Circular No. A-121 showed OMB that allocating costs had little effect on agencies' behavior; recovering costs means that actual transfers of funds will take place between suppliers and users of information technology facilities. Procedural aspects of the policy appear in Appendix II.

(17) Coordination with State and Local Governments. This policy reaffirms policy previously found in OMB Circular No. A-90, Transmittal Memorandum No. 1. The interagency group that worked on the revision of Circular No. A-90 recommended, and OMB agreed, that the Circular should be rescinded except for a single policy statement prohibiting Federal agencies from placing unnecessary restrictions on the information systems that State and local governments use to carry out federally financed program activities.

(18) Application of Up-to-date Information Technology. Recent availability of low cost, highly efficient and effective electronic information technology can greatly increase worker productivity and facilitate operation of Federal agency programs. The Circular states a predisposition, based in the Paperwork Reduction Act, in favor of applying such technology to the information life cycle within a responsible management context. Two broad areas of information technology merit further discussion: (1) electronic information collection and dissemination, and (2) end user computing.

- Electronic Collection and Dissemination of Information. Federal agencies are moving rapidly to provide for collection and dissemination of information through electronic media. In developing this Circular, OMB considered whether it was necessary to provide specific policies concerning electronic collection and dissemination of governmental information. OMB concluded that, except for the general predisposition in favor of applying new technological developments to information resources management, the policies that apply to information collection and dissemination in other media also apply to electronic collection and dissemination. It is important, however, that agencies recognize the necessity of systematically thinking through the application of policies stated elsewhere in this Circular to electronic collection and dissemination of information. For example, when developing electronic collection programs, agencies

should give particular attention to issues such as privacy, public access, and records management. When developing electronic dissemination programs, agencies should ensure that access is provided to each class of users upon reasonable terms, avoid problems arising from monopolistic control, ensure maximum reliance upon the private sector, and take necessary steps for cost accounting and cost recovery.

- End User Computing. Federal agencies are also moving rapidly to acquire end user computing capabilities. OMB endorses the managed innovation approach to end user computing presented in GSA's publication Managing End User Computing in the Federal Government (June 1983). Because end user computing places management of information in the hands of individual agency personnel rather than in a central automatic data processing organization, the Circular requires that agencies train end users in their responsibilities for safeguarding information; Appendix III deals in part with the security of end user computing.

Section 9. Assignment of Responsibilities.

This section assigns responsibilities for the management of Federal information resources addressed in this Circular. OMB Circular No. A-71 is rescinded and its contents are revised and incorporated into this section along with responsibilities assigned under the Paperwork Reduction Act; Section III of the Federal Property and Administrative Services Act, as amended; and Executive Order No. 12046. Certain assignments of responsibility from OMB to other agencies, as noted below, are also included. Following are principal noteworthy aspects of this section.

Responsibility for Managing Information Resources. Statement 9a(1) is a key element in the Circular because it establishes that the locus of responsibility for actual management of Federal information resources is the head of each agency. This means, for example, that the determination of what is "necessary for the proper performance of agency functions" with respect to information creation or collection (8a(1)) and information dissemination (8a(9)) lies with the head of the agency. In the Circular OMB sets the policy framework within which such determinations are to be made and the standards and provisions for reviewing the determinations, but the management decisions and their implementation belong properly with the agency holding the information resources.

Triennial Reviews. The Paperwork Reduction Act provides that the Director of OMB ". . . shall, with the advice and assistance of the Administrator of General Services, selectively review, at least once every three years, the information management activities of each agency to ascertain their adequacy and efficiency." (44 U.S.C. 3513) The Administrator of Information and Regulatory Affairs, OMB, and the Deputy Administrator of the General Services Administration, in an

exchange of correspondence dated June 13 and July 22, 1983, concurred that GSA has the necessary statutory authority to conduct reviews of Federal agency information resources management activities. Separate triennial reviews of agency activities by OMB and GSA would be unnecessarily duplicative, which would not be consistent with the Act. Accordingly, the triennial reviews conducted by GSA will be designed to meet OMB's requirements under the Paperwork Reduction Act as well as GSA's own needs.

Senior Officials for Information Resources Management. In accordance with 44 U.S.C. 3506(b) and 5 CFR 1320.8, agencies are required to designate a senior official to carry out responsibilities under the Paperwork Reduction Act. The designation of the official is intended to assure clear accountability for setting policy for agency information resources management activities, provide for greater coordination among the agency's information activities, and ensure greater visibility of such activities within the agency. The responsibilities of the senior official for information resources management were identified in OMB Bulletin No. 81-21, which has expired. Those responsibilities are now established in this Circular.

International Information Policy. The Circular deals with the management of information resources held by the Federal government. While the creation, collection, processing, transmission, dissemination, use, storage, and disposition of information by the Federal government has international ramifications, Federal government information resources management policy is not the same as "U.S. information policy," which refers to U.S. national interests in the information field vis-a-vis the policies and interests of other nations. The Circular formally acknowledges this distinction and assigns responsibilities for international information policy only insofar as it relates to Federal government information resources management policy.

Timely Technology Procurement. Inherent in effective management of information technology is the ability of program managers to acquire technology in a timely manner. GSA is assigned the responsibility in Section 9 to develop criteria that will streamline procurement procedures and delegate procurement authority to agencies that comply with those procedures. All Federal agencies are directed in Section 9 to develop internal policies and procedures that further provide for timely acquisition of information technology.

Records Management. The Paperwork Reduction Act makes the management of Federal records an integral part of information resources management. While no new policies are embodied in this Circular, responsibilities have been assigned in order to ensure that agency records management programs are considered within the context of Federal information resources management.

Section 10. Oversight.

The broad scope of the Circular dictates a strategy of focusing oversight on a series of aspects of information resources management rather than on a single comprehensive reporting scheme. OMB intends to use existing mechanisms, such as the fiscal budget, information collection budget, and management reviews, to examine agency compliance with the Circular. For example, during 1984 the management reviews for the FY 1986 budget year concentrated on five cross-cutting information issues: overall information resources management strategy, telecommunications, software management, "electronic filing," and end user computing. OMB issued data call bulletins requesting information specific to these issues, targeted the issues for special attention during the management reviews, and requested individual agencies to submit management improvement plans on specific aspects of the issues. Pursuit of this kind of selective oversight strategy permits OMB and the agencies the flexibility to shift the focus of oversight as information issues and the technological environment change.

**DEFINITIONS**

**Note:** The terms Automated Information System (AIS) and Automated Data Processing (ADP) System are often used interchangeably in the literature, including OMB Circular A-130, FIPS PUBS, Navy Security Manual, FAA Security Manual, and others. Generally, the term Automated Information Systems is broader in context than Automated Data Processing (ADP) systems, encompassing telecommunications systems and systems designed solely for word processing and/or electronic mail as well as traditional ADP systems. Since much of the guidance in this Manual is derived from other sources, including those noted above, the Manual may not always be consistent with respect to the usage of the terms AIS and ADP. This should not present any problems for the reader as the applicability of the guidance to either ADP or the broader concept of AIS can normally be taken from the context of the chapter, paragraph, or sentence. If there is doubt regarding the applicability of security requirements for a given system, good judgement should prevail when evaluating the acceptable level of risk. The requirements in this Manual are based primarily upon broad categories of system type and information sensitivity; more rigid standards and requirements may be adopted locally if the commanding officer determines the level of risk to warrant them.

The definition of the term Office Information System also varies considerably in the literature, but is defined rather specifically for the purposes of this Manual. Due to the rapid growth and integration of data processing, telecommunications, and office information systems in general, the simple categorization of information systems will continue to be a difficult if not impossible task.

**ACCEPTABLE LEVEL OF RISK** - A judicious and reasoned assessment by the appropriate Designated Approving Authority (DAA) that an automated information system (AIS) meets the provisions of this Manual and the minimum requirements of applicable security directives. The assessment should take into account the value of AIS assets, threats and vulnerabilities, countermeasures and their cost and effectiveness in compensating for vulnerabilities, and operational requirements.

**ACCESS** - An interaction between a person, process, or device and an object that results in the flow of information from one to another. An object is a passive entity that contains or receives information; e.g., records, files, directories, programs, processors, video displays, keyboards, printers, network nodes.

Note: Personnel who receive only computer output products from the automated system and do not input to or otherwise interact with the system (i.e., no "hands on" or other direct input or inquiry capability) are not considered to have AIS access and are accordingly not subject to the personnel security requirements of this manual. Such output products, however, shall either be reviewed prior to dissemination or otherwise determined to be properly identified as to content and classification.

**ACCESS CONTROL** - The process of limiting access to the resources of an AIS only to authorized persons, processes, or devices (including other AISs in a computer networks). Access control is accomplished through use of appropriate physical, administrative, and technical controls.

**ACCOUNTABILITY** - The quality or state which enables violations or attempted violations of AIS security to be traced to individuals who may then be held responsible.

**ACCREDITATION** - The official authorization that is granted to an AIS to process classified and/or sensitive information in its operational environment. Accreditation is based on the determination the AIS is operating at an acceptable level of risk, after a comprehensive security evaluation and consideration of other management factors (e.g., criticality of operations, cost to implement controls, impact on operations, planned changes in AIS operations.)

**ACTIVITY** - See AIS Activity.

**ADMINISTRATIVE SECURITY** (or Procedural Security) - The management constraints; operational, administrative, and accountability procedures; and supplemental controls established to provide an acceptable level of protection for data.

**ADP CLEARANCE** - Personnel classifications defined by the Office of Personnel Management which are assigned to civilian positions to indicate the level of trustworthiness required. Four designations (ADP I through ADP IV) are defined based on degree of involvement in computer system operation, sensitive application processing, AIS security management and other factors. See Clearance.

**ADP SECURITY OFFICER (ADPSO)** - See AIS Security Staff.

**ADP SYSTEM SECURITY OFFICER (ADPSSO)** - See AIS Security Staff.

**AIS** - Automated information systems include traditional ADP systems (mainframes and minicomputers), microcomputers, office information systems, networks which connect them, and applications (software) which run on them. It is any assembly of computer facilities, equipment, personnel, software, and administrative procedures configured for the purpose of classifying, sorting, calculating, computing, summarizing, storing, and retrieving data and information with a minimum of human intervention.

**AIS ACTIVITY** - Any operating or staff unit of the Coast Guard operating an AIS, or commercial firm providing AIS services to the Coast Guard under contract.

**AIS ASSET** (or Resource) - Any AIS facilities, equipment (computers, input/output devices, communication links), personnel, software, administrative procedures, supplies, or data/information used to support an automated process or function.

**AIS SECURITY DOCUMENTATION** - Documents which describe an activity's AIS security posture and include standard operating procedures, risk assessment plans and reports, security test and evaluation plans and reports, Inspector General (IG) reports and findings, incident reports, and contingency plans and test results.

**AIS SECURITY STAFF** - Individuals assigned responsibility for and who function as action officials for AIS security within their respective organization. An ADP Security Officer must be designated as a minimum at major commands (Headquarters' offices, area staffs, districts, and Headquarters' units); other staff designations provide for a hierarchy of responsibilities and may be assigned at the discretion of the commanding officer. Security staff designations include:

ADP Security Officer (ADPSO)
ADP Systems Security Officer (ADPSSO)
Network Security Officer (NSO)

**ANNUAL LOSS EXPECTANCY (ALE)** - The ALE of an AIS or activity is the expected yearly dollar value loss from the harm to the system or activity by attacks against its assets. The ALE is computed as part of the risk assessment.

**ATTACK** - The realization of a threat. Frequency of attack depends on such factors as the location, type, and value of information being processed. Short of moving the system or facility or radically changing its mission, there is usually no way that the level of protection can affect the frequency of attack. The exceptions to this are certain human threats where effective security measures can have a different effect. The fact that an attack is made does not necessarily mean that it will succeed. The degree of success depends on the vulnerability of the system or activity and the effectiveness of existing countermeasures.

**AUDIT** - An independent review and examination of systems records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, and to recommend any indicated changes in controls, policy, or procedures. An Internal Audit is conducted by personnel responsible to the management of the organization being audited. An External Audit is conducted by an organization independent of the one being audited.

**AUDIT TRAIL** - A set of records that collectively provide documentary evidence of processing used to aid in the reconstruction, review, and examination of the sequence of events leading towards a particular final result.

**AUTHENTICATION** - The process of establishing the validity of a claimed identity of a subject (person, process, or device) to verify the subjects eligibility to access specific AIS assets, most often categories of information.

**AUTHORIZATION** - The granting, to a person, process, or device, the right of access to an AIS asset. Authorization frequently refers to the right to access (read, write, modify, create, or delete) data.

**AUTOMATED INFORMATION SYSTEM (AIS)** - See AIS.

**BACKUP PLAN** - See Contingency Plan.

**BREACH** - The successful defeat of security controls which could result in a penetration of the system. Examples include: operation of user code in master code, unauthorized acquisition of identification password or file access passwords, accessing a file without using prescribed operating system mechanisms, and unauthorized access to tape library.

**BROWSING** - The act of searching through storage to locate or acquire information without necessarily knowing of the existence or the format of the information being sought.

**CALL BACK** (or Dial Back) - A procedure established for positively identifying a terminal dialing into a computer system by disconnecting the calling terminal and reestablishing the connection by the computer system's dialing the telephone number of the calling terminal.

**CENTRAL COMPUTER FACILITY** - One or more computers with their peripheral and storage units, central processing units, and communications equipment in a single controlled area. This does not include remote computer facilities, peripheral devices, or terminals which are located outside the single controlled area even though they are connected to the central computer facility by approved communication links.

**CERTIFICATION** - The official authorization that is granted to a sensitive application attesting to the adequacy of its security controls. Certification is made based on an independent review of security controls of the AIS facility and the application program and manual interfaces to determine if security design specifications are correct and have been properly implemented.

**CLASSIFICATION** - The determination that official information requires, in the interest of national security, a specific degree of protection against unauthorized disclosure, coupled with a designation signifying that such a determination has been made.

**CLASSIFIED INFORMATION** - Official information which requires protection against unauthorized disclosure in the interests of the national security of the United States, and which has been so designated in accordance with the provisions of Executive Order 12356. COMDTINST M5500.11 provides CG policy and guidance for the handling of Classified Information. See Confidential, Secret, and Top Secret.

**CLEARANCE** - An administrative determination by designated and competent authority that an individual is eligible for access to classified information of a specific classification category. Clearances apply to the right to access, on a need-to-know basis, classified information. See ADP Clearance.

**COMMANDING OFFICER** - Any head of a Coast Guard command or activity; division/branch or section chief; officer-in-charge or any other title assigned to an individual, military or civilian, who, through command status, position, or administrative jurisdiction, is the senior line management official for an AIS activity.

**COMMUNICATIONS SECURITY (COMSEC)** - The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. COMSEC includes cryptosecurity, transmission security, emission security, and physical security of communications security materials and information. COMDTINST M2000.3 provides guidance regarding CG communications security policy.

**COMPARTMENTATION** - The isolation of the operating system, user programs, and data files from one another in main storage in order to provide protection against unauthorized or concurrent access by other users or programs. Also the breaking down of sensitive data into small, isolated blocks for the purpose of reducing risk to the data.

**COMPROMISE** - The disclosure or loss of classified or sensitive information to persons not authorized access.

**COMPROMISING EMANATIONS** - Electromagnetic emanations that may convey data and, if intercepted and analyzed, may compromise sensitive information being processed by an AIS. TEMPEST is an unclassified short name referring to investigations and studies of compromising emanations. It is sometimes used synonymously for the term "compromising emanations".

**CONFIDENTIAL** - A Classification designation applied to information or material, the unauthorized disclosure of which could reasonably be expected to cause identifiable damage to the national security. Examples of "damage" include the compromise of information which indicates the strength of ground, air and naval forces in the United States and overseas areas; disclosure of technical information used for training, maintenance and inspection of classified munitions of war; revelation of performance characteristics, test data, design and production data on munitions or war.

**CONFIDENTIALITY** - A concept that applies to data that must be held in confidence and that describes the status and degree of protection that must be provided for such data about individuals as well as organizations.

**CONFIGURATION CONTROL** (or Configuration Management) - The use of procedures appropriate for controlling changes to a system's hardware and software structure for the purpose of ensuring that such changes will not lead to decreased data security.

**CONTINGENCY PLAN** - A contingency plan provides a course of action to be followed during or following an emergency or other abnormal event which causes or may cause a disruption in data processing services for essential functions (applications). Contingency plans address both the data processing support and the function itself. It is a comprehensive statement of all the actions to be taken before, during, and after a disaster (emergency condition), along with documented, tested procedures which, if followed, will ensure the availability of critical AIS resources and which will allow the continuity of operations.

**CONTROLS** (or Countermeasures or Safeguards) - The physical, personnel, administrative, hardware, software, or communications measure used to protect against unauthorized (accidental or intentional) disclosure, modification, or destruction of AISs and data, and denial of service to process data. Any action, device, procedure, technique, or other measure that reduces the vulnerability of an AIS or activity to the realization of a threat.

**COUNTERMEASURE** - See Controls.

**COVERT CHANNEL** - A communication channel that allows a process to transfer information in a manner that violates the system's security policy.

**DATA CHANNEL** - A hardware component which directs and controls the flow of data between main storage and input/output devices and allows the central processing unit (CPU) to operate concurrently with input/output operations.

**DATA CONFIDENTIALITY** - The state that exists when data is held in confidence and is protected from unauthorized disclosure. Misuse of data - by those authorized to use it for limited purposes - is also a violation of data confidentiality.

**DATA CONTAMINATION** - A deliberate or accidental act or process that results in a change in the integrity of the original data.

**DATA-DEPENDENT PROTECTION** - Protection of data at a level commensurate with the sensitivity level of the individual data elements, rather than with the sensitivity of the entire file which includes the data elements.

**DATA ENCRYPTION STANDARD (DES)** - The National Bureau of Standards (NBS) algorith, implemented in special purpose electronic devices, for the cryptographic protection of computer data. DES may be used for the protection of data that is sensitive or has a high value, and is vulnerable to unauthorized disclosure or undetected modification during transmission or while in storage.

**DATA INTEGRITY** - The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or intentional modification, disclosure, or destruction.

**DATA SET** - Logical name for a data file, used to eliminate reference to physical storage device.

**DATA TYPE (LEVELs I, II AND III)** - Three categories of data used to determine the degree of protection to be afforded data and automated information systems processing such data. This is a CG categorization which groups other recognized data/information categories for the convenience of prescribing automated information system security requirements.

a. Level I. Classified data.

b. Level II. Unclassified, sensitive data requiring special protection; for example, Privacy Act, For Official Use Only, technical documents restricted to limited distribution.

c. Level III. All other unclassified data.

**DEA SENSITIVE INFORMATION** (or Data) - Designation for information which requires a degree of protection, but does not meet the criteria for a confidential classification. Release could result in compromise of information or source and could result in the loss of life.

**DEDICATED MODE** - See Mode of Operation.

**DEGAUSS** - To apply a variable, alternating current (Ac) field for the purpose of demagnetizing magnetic recording media. The process involved increases the AC field gradually from zero to some maximum value and back to zero, which leaves a very low residue of magnetic induction on the media.

**DESIGNATED APPROVING AUTHORITY (DAA)** - The DAA is the official having responsibility for the accreditation of an AIS.

**DIAL BACK SYSTEM** - See Call Back.

**DISASTER PLAN** - See Contingency Plan.

**DISCLOSURE** (unauthorized) - The unauthorized release or access of Level I or II data to someone lacking proper clearance and a need-to-know. Also see Compromise.

**DISCRETIONARY ACCESS CONTROL** - A means of restricting access to objects based on the identity of subject (person, process, or device) and/or groups to which they belong. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject. For example, access control based on the basis of need-to-know are discretionary.

**DISTRIBUTED PROCESSING** - A general term, usually referring to the use of computers and/or intelligent (programmable) terminals at sites remote from a central computer facility. The trend is towards provision of some measure of local storage (e.g., diskette, cassette, or cartridge tape) and capabilities for file manipulation as well as data validation and computation within the context of distributed processing remote workstations.

**ELECTROMAGNETIC EMANATIONS** - Signals transmitted as radiation through the air and through conductors.

**EMERGENCY PLAN** - See Contingency Plan.

**ENCRYPT** - To convert plain text into unintelligible form by means of a cryptographic system which includes a set of mathematically expressed rules for rendering information unintelligence by effecting a series of transformations through the use of variable elements controlled by the application of a key to the normal representation of the information.

**FIRMWARE** - A method of organizing an automated system's control hardware in a microprogrammed structure rather than as wired circuitry such that the method falls in neither the software nor the hardware subsystems. It includes permanent or semi-permanent control coding at a micro-instruction level that implements a fixed application program, instruction set, I/O routine, operating routine, or other user-oriented function.

**FOR OFFICIAL USE ONLY (FOUO)** - Information designation assigned to unclassified official information of a privileged, proprietary, or personal nature which must be protected against unauthorized public release. Release of FOUO information must be accomplished in accordance with Freedom of Information Act directives.

**FRONT-END PROCESSOR** - A computer associated with a host computer that performs preprocessing functions such as line control, message handling, code conversion, error control, data control, data management, and terminal handling.

**HANDLED** (As in "Data is handled.") - Stored, processed or used in an automated information system or communicated, displayed, produced, or disseminated by an AIS.

**HANDSHAKING** - The exchange of control sequences to set up transmission.

**HARDWARE SECURITY** - Computer equipment features or devices used in an ADP system to preclude unauthorized accidental or intentional modification, disclosure, or destruction of AIS resources.

**INFORMATION SECURITY** (or Data Security) - The security that is required to assure the protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure, and that data is available when and where planned.

**INPUT/OUTPUT DATA CHANNEL** - See Data Channel.

**INTELLIGENCE** - The product resulting from the collection, evaluation, analysis, integration, and interpretation of all information concerning one or more aspects of foreign countries or areas, which is immediately or potentially significant to the development and execution of plans, policies, and operations.

**INTELLIGENT TERMINAL** - A terminal which includes a programmable processor and permits some level of processing rather than just emulation alone.

**LAW ENFORCEMENT INFORMATION** - Information pertaining to the enforcement of criminal laws. This includes information compiled to (a) prevent, control or reduce crime or to apprehend criminals; (b) identify individual criminal offenders; (c) conduct criminal investigations utilizing informants, witnesses and authorized technical aids; (d) maintain reports identifiable to an individual or organization at any stage of the process of enforcement of criminal laws.

**LEAST PRIVILEGE** - See Mode of Operation.

**LIMITED OFFICIAL USE (LOU)** - Information category used by the Department of State. LOU has the same handling and storage requirements as Confidential and must be encrypted when transmitted electronically between two sites.

**MANDATORY ACCESS CONTROL** - A means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (clearance) of subjects (person, process, or device) to access information of such sensitivity.

**MODE OF OPERATION** - The security environment and method of operating an automated information system or network. Modes include: Multilevel Security, Controlled Security, Systems High Security, Dedicated Security Mode, Periods Processing, and Least Privilege.

a. Multilevel Security Mode. Operation under an operating system (supervisor or executive) which permits various categories and types of classified information to be stored and processed concurrently in an AIS and which permits selective access to such information concurrently by personnel not cleared for the highest and most restrictive category of information in the system and users having the proper security clearances and need-to-know. The separation of personnel and information on the basis of security clearance and need-to-know is accomplished by the operating system and associated system software. Constraints may be placed on concurrent processing and storage by the Designated Approving Authority.

b. Controlled Security Mode. Operation of an AIS when at least some personnel (users) with access to the system have neither a security clearance nor a need-to-know for all classified material contained in the system. The separation and control of users and classified information on the basis of security clearance and security classification is accomplished by the implementation of security measures, i.e., personnel security, access controls, and the incorporation of firmware and software controls, which reduce or eliminate most system software vulnerabilities.

c. Systems High Security Mode. Operation of an AIS such that the central computer facility and all of its connected peripheral devices and remote terminals are protected in accordance with the requirements for the highest classification category and type of material contained in the system. All personnel having access to the system shall have a security clearance, but not necessarily a need-to-know, for all material contained in the system.

d. Dedicated Security Mode. Operation of an AIS such that the central computer facility, the connected peripheral devices, the communications facilities, and remote terminals are used and controlled exclusively by specific users or groups of users having a security clearance and need-to-know for the processing of classified or sensitive information. (Continued)

**MODE OF OPERATION** - (Continued)

e. Periods Processing Mode. The operation of an AIS such that various levels of security classification are processed at different times with the system being purged between periods.

f. Least Privilege Mode. The operation of an AIS such that each subject (person, process, or device) in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. Operation in this mode limits the damage that can result from accident, error, or unauthorized use.

**MULTILEVEL SECURITY** - See Mode of Operation.

**MULTIPROCESSING** - The capability in a computer system which contains two or more central processing units (CPUs). CPUs share information in two principal ways: 1) by sharing and using the same main storage and 2) by sharing and using the same input/output storage devices. Multiprocessing permits multiple users.

**MULTIPROGRAMMING** - The capability in a computer system that allows several jobs to share the resources of the system. System resources include: CPU time, main storage, input/output devices, and space on mass-storage volumes. Jobs usually co-reside in main storage and overflow to an auxiliary storage device, when necessary. Each job is given control of the central processing unit (CPU) according to a scheduling algorithm. Multiprogramming permits multiple users.

**MULTITASKING** - The capability in a computer system that allow two or more tasks (e.g., processing, input/output) to take place simultaneously. Multitasking does not permit multiple users.

**NATIONAL SECURITY INFORMATION** - Information or material, the unauthorized disclosure of which could reasonably be expected to cause damage to the national defense, and which usually bears a security classification.

**NATIONAL SECURITY-RELATED INFORMATION** - See Unclassified National Security-Related Information.

**NATO CLASSIFIED INFORMATION** - Information category encompassing all classified information, military, political and economic, circulated within and by NATO whether such information originates in the organization itself or is received from member nations of from other international organizations. See COMDTINST M5500.11.

**NEED-TO-KNOW** - The necessity for access to, knowledge of, or possession of certain information required to carry out official duties. Responsibility for determining whether a person's duties require that possession of or access to such information and whether the individual is authorized to receive it rests upon the individual having current possession, knowledge, or control of the information involved and not upon the prospective recipient(s).

**NETWORK** - The interconnection of two or more automated information systems that provide for the transfer or sharing of AIS resources. The AIS network consists of the central computer facilities, the remote terminals, the interconnecting communication links, the front-end processors, and the telecommunications systems.

**NETWORK SECURITY OFFICER (NSO)** - See AIS Security Staff.

**OBJECT** - A term used to denote passive entities that contain or receive information. Access to an object potentially implies access to the information it contains. Examples of objects are: records, blocks, pages, segments, files, directories, directory trees, and programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printer, network nodes, etc.

**OFFICIAL INFORMATION** - Information which is owned by, produced for or by, or is subject to the control of the United States Government. Three basic types of Official Information include: Classified, Privileged and Proprietary (often designated For Official Use Only), and Unclassified.

**OFFICE INFORMATION SYSTEM (OIS)** - Any electronic system designed and used solely for document management purposes; i.e., preparation (word processing), storage, retrieval, manipulation (sorting, indexing, etc.), and distribution (electronic mail). Office information system equipment excludes typewriters, office copy machines, and other devices which have no text editing capability.

**OPERATING SYSTEM (OS)** - An organized collection of programs and data that manage the resources of a computer system and facilitate the creation of computer programs and control their execution on that system. System resources include: CPU time, main storage, input/output devices, and space on mass-storage volumes. A multiprogramming OS is composed of control programs (for task management, job management and data management) and processing programs (for language processors and service programs). Terms such as monitor, executive, control program and supervisor are often used synonymously with operating system although they sometimes have a more specific meaning.

**PASSWORD** - A protected word or string of characters that identifies or authenticates a user for access to a specific resource such as a data set (file), or record.

**PENETRATION** - The successful identification and extraction of recognizable information from a protected data file or data set.

**PERSONAL INFORMATION** (or Data) - Any item of information about a person that is not a matter of public record and is usually considered to be personal to an individual. It includes but is not limited to: social security number (SSN), information about the individual's financial, family, social, and recreational affairs, the individual's medical, educational (except military training), employment, political, or criminal history, information that identifies, describes, or gives a basis for inferring personal characteristics.

**PERSONNEL SECURITY** - The procedures established to ensure that each individual has a background which indicates a level of assurance of trustworthiness which is commensurate with the value of AIS resource which the individual will be able to access, and ensures that the employment and retention of selected Coast Guard military and civilian personnel is clearly consistent with the interests of national security.

**PHYSICAL SECURITY** - The protection of assets from disruption of their safe and secure state. Physical security includes the application of physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, facilities, material, and documents, and to safeguard them against espionage, sabotage, damage, and theft. Protection against all physical threats to the central computer facility, its remote computer and terminal facilities, the related tape/disk libraries, and the supporting area achieved by locks, guards, badges, alarm systems, facility construction standards, etc. Associated with these measures are provisions for protecting the AIS facility from natural or other environmental hazards and contingency planning.

**PLAIN TEXT** - Intelligible text or signals that have meaning and that can be read or acted upon without the application of any decryption.

**PRIVACY** - The right of an individual to determine for himself when, how, and to what extent information about him can be obtained or communicated to others. Privacy also includes the right of individuals to know that recorded information is accurate, pertinent, complete, up-to-date, and reasonably secure from unauthorized access, either accidental or intentional.

**PRIVACY INFORMATION** - Personal information which relates to individual US citizens as provided by the Privacy Act of 1974.

**PRIVILEGED INFORMATION** - Information requiring protection for conformance with business standards or as required by law; e.g., government-developed information involving the award of contracts. Privileged information is designated as For Official Use Only.

**PROPRIETARY INFORMATION** - Information requiring protection to protect software or data in conformance with a limited rights agreement or which is the exclusive property of a civilian corporation or individual and which is on loan to the Government for evaluation or for its proper use in adjudicating contracts. Proprietary information is designated as For Official Use Only.

**RECORDS** - Information registered in either temporary or permanent form so that it can be retrieved, reproduced, or preserved.

**RESOURCE-SHARING COMPUTER SYSTEM** - A computer system which uses its resources, including input/output (I/O) devices, storage, central processor (arithmetic and logic units), control units, and software processing capabilities, to enable one or more users to manipulate data and to process co-resident programs in an apparently simultaneous manner. The term includes systems with one or more of the capabilities commonly referred to as timesharing, multiprogramming, multi-accessing, multiprocessing, or concurrent processing.

**RESTRICTED AREA** (or Control Zone or Security Perimeter) - The space that surrounds AIS equipment that is used to process classified or sensitive information and that is under sufficient physical, administrative, and technical control to preclude an unauthorized entry or successful hostile intercept of compromising emanations from within this space.

**RESTRICTED DATA** - Data relating to Atomic Energy Materials (See DOT 1630.2).

**RISK** - The chance of or exposure to loss.

**RISK ASSESSMENT** (or Risk Analysis) - An analysis of assets and vulnerabilities, and threats to those assets to determine the level of risk to an AIS. Risk is "measured" either quantitatively or qualitatively by determining the impact of threats on the facility, system, information, personnel, and supported organizations or other users.

**SECRET** - A Classification designation applied only to information or material the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security. Examples of "serious damage" include disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans or intelligence operations; compromise of significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to the national security.

**SECURITY** - The effectiveness level of the controls which allow access to an AIS such that only properly authorized individuals, or processes operating on their behalf, will have access to read, write, create, or delete information, or interfere with the timely processing of information.

Also the measures required to protect against unauthorized (accidental or intentional) disclosure, modification, or destruction of AISs and data, and denial of service to process data. Components include Physical Security, Administrative Security, Personnel Security, and Technical Security (hardware, software, and communications). See definitions for each item listed.

**SECURITY TEST & EVALUATION (ST&E)** - An examination and analysis of the security features of an AIS activity or network as they have been applied in an operational environment to determine the security posture of the activity or network upon which an accreditation can be based.

**SENSITIVE APPLICATION** - The set of procedures (predominantly but not necessarily exclusively automated) which define the arithmetic computations and data handling operations of classified (Level I) or sensitive (Level II) data to achieve a specific purpose. An application has automated processes programmed in a language (e.g., assembly, BASIC, COBOL, Wang glossary) or off-the-shelf application package which permits automatic processing of the information. Text files or data base files containing (storing) but not processing sensitive information are not sensitive applications.

**SENSITIVE INFORMATION** (or Data) - Information that, as determined by a competent authority, must be protected because its unauthorized disclosure, alteration, loss, or destruction will at least cause perceivable damage to someone or something. Classified information, which is also sensitive information, is always designated as classified.

**SENSITIVE INFORMATION** - (Continued)

An abbreviated designation commonly used for unclassified, sensitive information This type of information includes, but is not limited to, certain personal, budget, financial and management information, and information generally categorized as For Official Use Only (e.g., proprietary and privileged information). A generic designation for unclassified information that must be protected from unauthorized disclosure, alteration, loss, or destruction because it would cause perceivable damage to someone or something. This type of information includes but is not limited to certain personal, budget, financial and management information, and information generally categorized as For Official Use Only (e.g., proprietary and privileged information).

**SPECIAL ACCESS PROGRAM** - Any program imposing need-to-know or related security requirements or constraints which are beyond those normally provided for the protection of Classified Information (Confidential, Secret, or Top Secret). Constraints may include, but are not limited to, special clearance, adjudicative, or investigative requirements, special designation of officials authorized to determine need-to-know, or special lists or briefings of persons determined to have a need-to-know. Sensitive Compartmented Information (SCI) and Atomic Energy Material are examples of Special Access Programs.

**SUBJECT** - A term used to denote an active entity, generally in the form of a person, process, or device that causes information to flow among objects or changes the system state.

**SYSTEM HIGH SECURITY** - See Mode of Operation.

**TECHNICAL SECURITY** - The hardware, software, and communications features of a system which, in concert with Physical Security and Administrative Security controls, provide an acceptable level of protection for data.

**TELECOMMUNICATIONS** - Any transmission, emission, or reception of signs, signals, writing, images, sounds, or other information by wire, radio, visual, or any electromagnetic systems.

**TEMPEST** - The study and control of spurious electronic signals emitted from electrical equipment. See Compromising Emanations.

**THREAT** - The source of an adverse event that can cause a loss. Threats are categorized as either natural hazards, accidents, and intentional acts. (Continued)

**THREAT** - (Continued)

Any circumstance or event with the potential to cause harm to the automated information system or activity in the form of destruction, disclosure, and modification of data, or denial of service. A threat is a potential for harm. The presence of a threat does not mean that it will necessarily cause actual harm. Threats exist because of the very existence of the system or activity and not because of any specific weakness. For example, the threat of fire exists at all facilities, regardless of the amount of fire protection available.

**TOP SECRET** - A classification designation applied only to information or material the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security. Examples of "exceptionally grave damage" include armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital national defense plans or complex cryptologic and communications intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technological developments vital to the national security.

**TRUSTED COMPUTER SYSTEM** - A system that employs sufficient hardware and software integrity measures to allow its use for processing simultaneously a range of sensitive and/or classified information. The National Computer Security Center has defined application-independent evaluation criteria to classify systems into four broad hierarchical divisions of enhanced security protection with varying degrees of trust.

**UNCLASSIFIED NATIONAL SECURITY-RELATED INFORMATION** - Unclassified political, economic, military, and special subjects (e.g., human, rights, technology) information which has been determined to have value to foreign adversaries. See NCSC-11.

**USER** - A person or organization receiving products or services produced by an automated system either by access to the system or by other means.

**VITAL RECORDS** - Records essential to the continued functioning of an organization during and after an emergency, and also those records essential to the protection of the rights and interests of that organization and of the individuals for whose rights and interests it has responsibility. See Federal Emergency Operating Records and Federal Rights and Interests Records.

**VOLUME** - The standard unit of auxiliary storage, such as magnetic tape reel or disk pack.

**VULNERABILITY** - A weakness in the physical layout, organization, procedures, personnel, management, administration, hardware, or software that may be exploited to cause harm to the automated information system or activity. The presence of a vulnerability does not in itself cause harm; a vulnerability is merely a condition or set of conditions that may allow the AIS or activity to be harmed by an attack.

**WIRETAP**

Active Wiretap: The attaching of an unauthorized device, such as a computer terminal, to a communications circuit for the purpose of obtaining access to data through the generation of false messages or control signals, or by altering the communications of legitimate users.

Passive Wiretap: The monitoring and/or recording of data while the data is being transmitted over a communication link.

**AIS SECURITY REFERENCES**

**A. COMMANDANT INSTRUCTIONS.**

1. COMDTINST M2000.3A, Telecommunications Manual (G-TTS)

2. COMDTINST M5212.12, Paperwork Management Manual (G-CMA)

3. COMDTINST 5230.23, Use of Computers Aboard CG Cutters (G-TES)

4. COMDTINST 5230.24, Information Resource Management System Acquisition Authority (G-TDS)

5. COMDTINST 5230.26, Small Information Resources Management (IRM) Systems Acquisition Documentation (10 Step) (G-TDS)

6. COMDTINST M5233.3, ADP Management Manual

7. COMDTINST M5234.2, Automated Data Systems (ADS) Documentation Standards (G-TDS)

8. COMDTINST M5260.2, Privacy and Freedom of Information Acts Manual (G-CMA)

9. COMDTINST M5500.11A, Security Manual (G-OIS)

10. COMDTINST C5510.7, Coast Guard Policy on Control of Compromising Emanations (U) (G-TTS)

11. COMDTINST 5510.10, Civilian Personnel Security Program (G-PS)

12. COMDTINST M5510.16, Military Personnel Security Program (G-PS)

13. COMDTINST 5510.18, Classification Guide for Information Concerning International Drug Trafficking (G-OIS)

14. COMDTINST M5527.1, Investigations Manual (G-OIS)

15. COMDTINST M5700.7, Internal Control Systems Program (A-123) (G-CMA)

**B. OFFICE OF MANAGEMENT AND BUDGET (OMB) CIRCULARS.**

1. OMB Circular A-123, Internal Control Systems

2. OMB Circular A-130,, Management of Federal Information Resources

**C. NATIONAL BUREAU OF STANDARDS (NBS) FEDERAL INFORMATION PROCESSING STANDARDS (FIPS).**

1. FIPS PUB 31, Automatic Data Processing Physical Security and Risk Management

2. FIPS PUB 38, Guidelines for Documentation of Computer Programs and Automated Data Systems

3. FIPS PUB 39, Glossary for Computer Systems Security

4. FIPS PUB 41, Computer Security Guidelines for Implementing the Privacy Act of 1974

5. FIPS PUB 46, Data Encryption Standard

6. FIPS PUB 48, Guidelines on Evaluation of Techniques for Automated Personal Identification

7. FIPS PUB 64, Guidelines for Documentation of Computer Programs and Automated Data Systems for the Initiation Phase

8. FIPS PUB 65, Guidelines for Automated Data Processing Risk Analysis

9. FIPS PUB 73, Guidelines for Security of Computer Applications

10. FIPS PUB 74, Guidelines for Implementing and Using the NBS Data Encryption Standard

11. FIPS PUB 81, DES Modes of Operation

12. FIPS PUB 83, Guidelines on User Authentication Techniques for Computer Network Access Control

13. FIPS PUB 87, Guidelines for Automated Data Processing Contingency Planning

**C. NATIONAL BUREAU OF STANDARDS (NBS) FEDERAL INFORMATION PROCESSING STANDARDS (FIPS) (Cont'd)**

14. FIPS PUB 88, Guideline on Integrity Assurance and Control in Database Administration

15. FIPS PUB 94, Guideline on Electrical Power for ADP Installations

16. FIPS PUB 101, Guidelines for Lifecycle Validation, Verification, and Testing of Computer Software

17. FIPS PUB 102, Guidelines for Computer Security Certification and Accreditation

18. FIPS PUB 112, Standard on Password Usage

19. FIPS PUB 113, Standard on Computer Data Authentication

20. FIPS PUB 121, Guidance on Planning and Implementing Computer System Reliability

**D. OFFICE OF PERSONNEL MANAGEMENT (OPM) DIRECTIVES.**

Federal Personnel Manual

1. Chapter 731 - Personnel Suitability

2. Chapter 732 - Personnel Security

**E. MISCELLANEOUS.**

1. Federal Fire Council Recommended Practice No. 1, Fire Protection for Essential Electronic Equipment

2. RP-1, Standard Practice for the Fire Protection of Essential Electronic Equipment Operations

3. NFPA Standard No. 75, Protection of Electronic Computer/Data Processing Equipment

4. FIRMR 201-6, Protection of Personal Privacy

5. FIRMR 201-7, Security of Information Resources System

6. FIRMR 201-30, Management of ADP Resources

7. FIRMR 201-32, Contracting for ADP Resources

**E. MISCELLANEOUS (Cont'd).**

8. FIRMR 201-38, Management of Telecommunications Resources

9. FIRMR 201-40, Contracting for Telecommunications Resources

10. FIRMR 201-45, Management of Records

11. DoD 5220.22, Industrial Security Program

12. DoD 5200.1-R, Information Security Program Regulation

13. Department of Defense Trusted Computer System Evaluation Criteria

**RISK ASSESSMENT FOR OTHER MICROCOMPUTERS & OFFICE INFORMATION SYSTEMS**

There are many microcomputers other than the Standard Terminal being used throughout the Coast Guard; this section addresses the need to evaluate the security of these devices.

To begin the risk assessment, the reviewer should identify the value and criticality of the system (hardware, software, and data) which is at risk. Criticality is the importance of the system to mission performance. The first part of this enclosure provides forms that can be used to document the value and criticality of the system. These forms are provided as an example of a means of gathering the necessary information that will factor into the reviewers decisions concerning the vulnerability and risk to the system. The reviewer use these or any other means deemed appropriate.

After system value and criticality is determined, the reviewer should apply the second part of this enclosure, the SECURITY CHECKLIST. The checklist should be applied to each unique office system just as the survey was in part one. The qualitative nature of the checklist lends itself to the lower dollar value associated with most microcomputer based office systems as compared to the more expensive mini and mainframe systems where a quantitative analysis is justified. There are no "correct" answers for any of the checklist questions and not all questions will necessarily apply to all systems. When complete, the checklist should be reviewed and questions that were answered "no" should be given closer scrutiny. The narrative that follows the checklist is provided to assist the reviewer in evaluating those questions answered "no" in relation to his knowledge of the system being examined and the needs and resources of the office using the system.

The conclusions and decisions reached on the security and vulnerability of the office microcomputer system, will rely heavily on the knowledge and expertise of the reviewer. The checklist, as with any tool or aid, provides a means of organizing the examination process and hopefully, alerting the reviewer to areas where more in depth review and research may be required. The items outlined in the checklist are by no means comprehensive nor necessarily relevant to all systems. The decisions of how much security and to what degree needed to protect certain assets is left up to the reviewer to determine for each unique set of circumstances.

**OFFICE INFORMATION SYSTEM (OIS) SECURITY SURVEY**

1. The following forms are taken from a computer survey that was conducted by headquarters personnel in 1985. They are being provided in this enclosure because the information supplied to complete them will lay a basic framework for assessing a value and awareness of the assets of the microcomputer system(s) under evaluation.

2. Complete the survey for each separate office system/cluster. The completed surveys should be marked "For Official Use Only." Completed forms should be retained by the activity's ADP System Security Officer (ADPSSO).

INSTRUCTIONS FOR COMPLETION
OF THE
OIS SECURITY SURVEY
OVERVIEW
PART I

SECTION I -- SUMMARY INFORMATION.

1. Provide the English name by which the system is identified. This name should be the accepted and recognized name used at the activity.

2. Self-explanatory.

3. Use the figure of $2.50 per line of code when computing the cost of an application program.

4. Identify the primary purpose which the system serves--its reason for existence.

5. Identify by name, the OIS Security Officer or the System Manager. If an individual has not been appointed, identify the person to whom questions should be directed.

6. Self-explanatory.

SECTION II -- STATUS OF ACCREDITATION SUPPORT DOCUMENTATION.

1. Self-explanatory.

SECTION III -- SYSTEM PROFILE.

1. Self-explanatory.

SECTION IV -- OPERATING SYSTEM/APPLICATION SOFTWARE.

1. Provide the name of the operating system such as MVS, CTOS, and the version number.

SECTION V -- SYSTEM DATA.

1. Please do not identify the data by name. Just place a check by all that are applicable.

INSTRUCTIONS FOR COMPLETION
OF THE
OIS SECURITY SURVEY
OVERVIEW
PART I

VI -- OPERATING HOURS.

1. Prime shift is defined as the normal working day in terms of the traditional 0800-1600 or similar workday. Secondary shift would be the one following the prime shift such as 1600-2400.

   Remote access inhibit capability is similiar to the "Disable Cluster" on the Standard Terminal. When the inhibit capability is "on", no remote device can access the CPU or main storage.

SECTION VII -- REMOTE USER/COMMUNICATIONS CAPABILITY.

1. Self-explanatory.

2. A remote user is defined as any terminal or system not physically located in the room housing the Master Workstation.

   A. Includes both hard-wired and dial-up users.

   B. Self-explanatory.

   C. Hard-wired users are connected directly to the central CPU and are not required to dial-up.

   D. Dial-up access is obtained either through the use of a data phone or an acoustical coupler modem.

3. Identify what public communication network(s) are used with the system, such as GTE TELENET, TYMNET, etc.

4. Identify what public communication network(s), such as ARPANET, Defense Data Network (DDN), etc.

5. Identify any other networks used by the system including local area networks.

INSTRUCTIONS FOR COMPLETION
OF THE
OIS SECURITY SURVEY
OVERVIEW
PART I

SECTION VIII -- HARDWARE/SOFTWARE SECURITY COUNTERMEASURES.

1. Self-explanatory.

2. Identify the levels of password protection used and/or available on the system.

3. Briefly describe the steps which are required to sign-on and access a file or program at the central CPU.

SECTION IX -- SYSTEM RELIABILITY.

1. Self-explanatory.

2. Self-explanatory.

SECTION X -- SURVEY PREPARATION INFORMATION.

1. Self-explanatory.

INSTRUCTIONS FOR COMPLETION
OF THE
OIS SECURITY SURVEY
OVERVIEW
PART II

(NOTE: PLEASE REVIEW THE ATTACHED EXAMPLES
BEFORE STARTING SCHEMATICS)

(NOTE: IF THIS INFORMATION ALREADY EXISTS ON SOME OTHER FORM,
DO NOT REDO BUT PUT A LEGIBLE COPY IN THE SURVEY FILE.)

SECTION I -- ORGANIZATIONAL STRUCTURE.

Provide an organizational chart.

SECTION II -- SYSTEM CONFIGURATION DIAGRAM.
This is a block diagram showing all the components of a system. It is not meant to reflect a floor plan. The diagram should represent all equipment associated with hosts, OISs, standalones, clusters, networks. Each block should show the name of the piece of equipment, its model number, its communication capability, the telecommunication transfer rate, its storage capacity (if applicable), its interface with other equipment, the room number where it's located, and the routing symbol of the custodian.

SECTION III -- HARDWARE DATA.

1. List the system components.
   If this information exists on another form at the activity, do not transfer the information but attach a legible copy.

AUTOMATED INFORMATION SYSTEM (AIS)
OFFICE INFORMATION SYSTEM SECURITY SURVEY
PART I

SECTION I. SUMMARY INFORMATION. (Applies to each separate Office Information System. This survey form should be reproduced for the number of systems at the activity.)

1. System Identification: (The name by which the system is known at the activity but not necessarily the manufacturer's make or model.)

   _____

2. Manufacturer's Identification: (The make, model and other pertinent information.)

   _____

   _____

3. Total value of system: $ _____ (Dollar value should reflect impact of loss and cost to replace. If actual figures are not available, an estimate will suffice. The total value of system equals A + B below.)

   A. Equipment: $ _____

   B. Software: $ _____ (Operating system, system software and proprietary systems.)

4. Mission relatedness/criticality. Primary function(s) of the system:

   _____

   _____

   _____

   _____

   _____

   _____

OFFICE INFORMATION SYSTEM SECURITY SURVEY
PART I

SECTION I. SUMMARY INFORMATION. (Cont'd)

5. ADP System Security Officer: (If none designated, then the System Manager or other responsible individual.)

Name: _____

Mailing _____

Address: _____

_____

_____

_____

Telephone: (FTS) _____

(Commercial) _____

Normal Working Hours: _____

6. Title (This should not be confused with the individual's official title such as Computer Programmer, Budget Analyst, Section Chief, etc.)

( ) ADP System Security Officer

( ) System Manager

( ) Other _____

SECTION II. STATUS OF ACCREDITATION SUPPORT DOCUMENTATION. (Applies to each ADP system.)

1. Check all documentation that currently exists:

( ) Activity AIS Security Plan

( ) Risk Assessment

( ) Standard Operating Procedures

( ) System Security Procedures

( ) Contingency Plan

Date of plan or last change is _____

OFFICE INFORMATION SYSTEM SECURITY SURVEY
PART I

SECTION III. SYSTEM PROFILE.

1. Check all that apply:

( ) The OIS handles Level II unclassified sensitive data. See Section V, System Data

( ) The OIS is a shared logic system with more than one simultaneous user not having need-to-known for all data within the system.

( ) The OIS Security Operating Procedures have been documented and approved.

( ) A list of the operating countermeasures is attached.

( ) These countermeasures provide proper data protection and audit trails.

( ) These countermeasures do not provide data protection and audit trails.

( ) Password protection or other equivalent countermeasures are employed for system access and for individual file access.

( ) The OIS handles Level III unclassified non-sensitive data only.

SECTION IV. OPERATING SYSTEM/APPLICATION SOFTWARE.

1. Operating system and version number:

Operating System: _____

OFFICE INFORMATION SYSTEM SECURITY SURVEY
PART I

SECTION V. SYSTEM DATA.

1. Categories of information: (Place a check mark ( ) beside each category of information that is processed on system.)

LEVEL I.

A. NATIONAL SECURITY INFORMATION

1. Confidential_____
2. Secret_____
3. Top Secret_____
4. Sensitive Compartment_____
5. NATO_____
6. DOE-Restricted Data_____

LEVEL II.

B. NATIONAL SECURITY-RELATED INFORMATION_____

C. SENSITIVE INFORMATION

1. For Official Use Only (FOUO)_____
2. Vital Records_____
3. Proprietary_____
4. Privacy_____
5. Financial_____
6. Sensitive management_____
7. Privileged_____
8. DEA Sensitive_____
9. Limited Official Use (Dept. of State)_____
10. Law Enforcement_____
11. Attorney/Client_____
12. Doctor/Patient_____
13. Cleric/Penitent_____
14. Other_____
(Specify generic label)

LEVEL III.

D. OTHER INFORMATION

1. Administrative_____
2. Operations_____
3. Command/Control_____
4. Engineering_____
5. Planning_____
6. Property_____

OFFICE INFORMATION SYSTEM SECURITY SURVEY
PART I

SECTION VI. OPERATING HOURS.

1. Master Work Station is (check all that are applicable):

( ) Operational and staffed during prime shift and then secured.

( ) Operational and staffed during prime shift and then left operating unmanned.

( ) Operational and unmanned during prime shift and then secured.

( ) Operational and unmanned 24 hours a day.

( ) Is never powered down and does not have remote access inhibit capability.

( ) Is never powered down but has remote access inhibit capability.

( ) Is never operational on weekends.

SECTION VII. REMOTE USER/COMMUNICATIONS CAPABILITY.

1. Total number of system users (personnel): _____

2. Remote users (For Clusters Only. Terminals not in the same physical room as the Master Workstation):

A. Total number of remote workstations: _____

B. Average number of remote workstations on-line at one time: _____

C. Number of workstations hardwired to system: _____

D. Number of workstations with dial-up access: _____

3. Public packet switching communications network used:

_____

4. Private packet switching communications network used:

_____

5. Other communications networks used (Identify name and type of network.):

_____

OFFICE INFORMATION SYSTEM SECURITY SURVEY
PART I

SECTION VIII. HARDWARE/SOFTWARE SECURITY COUNTERMEASURES.

1. Password Protection:

( ) The system has the capability of password protection and passwords are a mandatory requirement.

( ) The system has the capability of password protection but passwords are an optional requirement.

( ) The system has the capability of password protection but does not have it implemented.

( ) The system does not have the capability of password protection.

2. Type of password protection used or available: (Check all that are applicable.)

( ) System access password protection.

( ) File/document access password protection.

( ) Other _____

3. Access requirements. (Describe the access process of the system.)

_____

_____

_____

_____

_____

OFFICE INFORMATION SYSTEM SECURITY SURVEY
PART I

SECTION IX. SYSTEM RELIABILITY.

1. Supply the maximum time system may be down without causing adverse impact:

   a. Minor adverse impact _____ hours

   b. Major adverse impact _____ hours

2. Provide information for the following categories of confirmed/suspected incidents during the past six months. Attach an additional sheet if necessary.

   a. Loss of system availability.

   b. Destruction/Modification of data.

   c. Others (e.g., known unauthorized disclosures of data.)

SECTION X. SURVEY PREPARATION INFORMATION.

1. Survey prepared by:

   Name: _____

   Title:_ _____

   Address: _____

   _____

   _____

   _____

   Telephone: __(  )_____

   Signature of Preparer _____

   Date _____

OFFICE INFORMATION SYSTEM SECURITY SURVEY
PART II

SECTION I. ORGANIZATIONAL STRUCTURE: (Show organizational structure of the activity. Indicate organizational element responsible for system. If system is physically located outside the element having responsibility, identify element who has physical custody.)

OFFICE INFORMATION SYSTEM SECURITY SURVEY
PART II

SECTION II. SYSTEM CONFIGURATION DIAGRAM: (Show all major equipment (processing units, terminals, peripherals, etc.) and their interface. Use additional sheets of paper as required.

OFFICE INFORMATION SYSTEM SECURITY SURVEY
PART II

SECTION III. HARDWARE DATA.

1. System description: (List all components, master station, peripherals, communications processors, encryption devices, remote devices, network and remote interfaces. Be specific with exact quantities. Serial numbers are not required. If this information is on another form at the activity, do not transfer the data but provide a legible copy.)

| | TYPE OF EQUIPMENT | |
|---|---|---|
| MANUFACTURER'S NAME | MAKE AND MODEL | QUANTITY |
| _____ | _____ | _____ |
| _____ | _____ | _____ |
| _____ | _____ | _____ |
| _____ | _____ | _____ |
| _____ | _____ | _____ |
| _____ | _____ | _____ |
| _____ | _____ | _____ |
| _____ | _____ | _____ |
| _____ | _____ | _____ |
| _____ | _____ | _____ |
| _____ | _____ | _____ |
| _____ | _____ | _____ |
| _____ | _____ | _____ |
| _____ | _____ | _____ |
| _____ | _____ | _____ |

(Use additional sheets if needed)

# SECURITY CHECKLIST
# FOR
# MICROCOMPUTERS OTHER THAN
# COAST GUARD STANDARD TERMINAL

| **ADMINISTRATIVE** | **YES** | **NO** | **N/A** |
|---|---|---|---|
| 1) Does your office own the computer that is being used by your office staff? | ___ | ___ | ___ |
| 2) Is there a policy requiring users of the computer to periodically change their passwords? | ___ | ___ | ___ |
| 3) Are there policies with regards to the sensitivity of the data stored and processed on the computer? | ___ | ___ | ___ |
| 4) Has a system administrator been appointed for the computer system? | ___ | ___ | ___ |
| 5) Is there an ADP System Security Officer (ADPSSO) assigned for the computer system? | ___ | ___ | ___ |
| 6) Are all the users of the computer system known to the system and to the system administrator? | ___ | ___ | ___ |
| 7) Are there procedures for the numbering and tracking of floppy disks for your system? | ___ | ___ | ___ |
| 8) Are there procedures in place, known to system users, to report theft of computer or peripheral devices? | ___ | ___ | ___ |

| **DOCUMENTATION** | **YES** | **NO** | **N/A** |
|---|---|---|---|
| 1) Are there copies of computer operational manuals for the equipment? | ___ | ___ | ___ |
| If so, are they up to date and complete? | ___ | ___ | ___ |
| 2) Are specific system or operational procedures documented and available for users to reference? | ___ | ___ | ___ |
| 3) If the computer is accessed by multiple users, is an access log maintained to account for who, when, and for how long the computer was being used? | ___ | ___ | ___ |
| 4) Are there procedures or standards for documenting system and program changes? | ___ | ___ | ___ |
| If so, are they adhered to by facility personnel? | ___ | ___ | ___ |
| 5) Is there a current list of all data files, applications software, and system software on the computer system for inventory and recovery purposes? | ___ | ___ | ___ |
| 6) Is there a current list of all hardware comprising the computer system (serial numbers, model numbers, board numbers, memory size, etc.) for inventory and recovery purposes? | ___ | ___ | ___ |

| **PHYSICAL** | **YES** | **NO** | **N/A** |
|---|---|---|---|
| 1) Is the computer readily accessible by anyone in the office area? | ___ | ___ | ___ |
| 2) Is access to the office area where the computer is located controlled (locked) during off-hours? | ___ | ___ | ___ |
| 3) Does the janitorial staff have access to the area where the computer is located during the off-hours? | ___ | ___ | ___ |
| 4) Is the computer physically secured to a desk or work table? | ___ | ___ | ___ |
| 5) Does the computer have a key lock or some device to deny access to the power switch when not in use? | ___ | ___ | ___ |
| 6) If the keyboard is not an integral feature of the computer cabinet, is it securely attached to the cabinet? | ___ | ___ | ___ |
| 7) Are computers positioned so their screens cannot be easily seen by other people aside from the user? | ___ | ___ | __ |
| 8) If a printer is part of the system configuration, is it secured to a desk or work table? | ___ | ___ | ___ |
| 9) Does printer location allow ready viewing of printouts by anyone in office area? | ___ | ___ | ___ |
| 10) If a separate media storage device (tape unit, hard disk) is part of the system configuration, is it located in an area of limited access? | ___ | ___ | ___ |
| 11) Are all cables connecting the equipment in the system configuration run or hung in accordance with applicable building codes and regulations? | ___ | ___ | ___ |
| 12) Are dust/protective covers provided and used on computer and peripheral components? | ___ | ___ | ___ |
| 13) Is the area where the computer is located covered by an area fire extinguishing system? | ___ | ___ | ___ |
| 14) If the office area is equipped with an overhead sprinkler system, does the position of the computer expose it to the spray area of a sprinkler head? | ___ | ___ | ___ |

| | YES | NO | N/A |
|---|---|---|---|
| 15) Is there a means of preventing unauthorized access to the inside of the computer cabinet (to prevent theft of boards or components)? | ___ | ___ | ___ |
| 16) Is some form of government identification label placed on the computer and peripheral devices? | ___ | ___ | ___ |
| 17) Does the location of your activity place it in an area with a reasonable likelihood of a natural disaster occurring (hurricane, earthquake, flooding, etc.) which might damage the computer? | ___ | ___ | ___ |
| 18) Is there an overall building security system or procedures in place at the computer site? | ___ | ___ | ___ |
| 19) If the computer system uses a key to control power or machine access, is there a person or procedure for controlling access to the key(s)? | ___ | ___ | ___ |
| 20) If the computer is secured to a work space or cabinet arrangement, are there wheels or casters to allow it to be moved? | ___ | ___ | ___ |

| **ENVIRONMENTAL** | **YES** | **NO** | **N/A** |
|---|---|---|---|
| 1) Is the computer located where it is directly exposed to sunlight? | ___ | ___ | ___ |
| Extreme heat? | ___ | ___ | __ |
| Extreme cold? | ___ | ___ | ___ |
| 2) Is there an approved class fire extinguisher readily accessible in the area where the computer is located? | ___ | ___ | ___ |
| 3) Is there adequate ventilation around the computer and any peripheral devices to prevent heat buildup? | ___ | ___ | ___ |
| 4) Are there smoke/fire detectors in the immediate area of the computer? | ___ | ___ | ___ |
| 5) Are computer cables and power cords arranged and maintained so as not to pose a fire hazard or safety hazard to personnel? | ___ | ___ | ___ |
| 6) Is the area where the computer is located equipped with raised flooring? | ___ | ___ | ___ |
| 7) Does the electrical circuit the computer is plugged into carry a sufficient current for the equipment to operate on? | ___ | ___ | ___ |
| 8) Is there a voltage surge suppressor or regulator installed to protect the computer and peripheral devices from power spikes or surges? | ___ | ___ | ___ |
| 9) Are there frequent, observable power interruptions on the circuit that the computer is connected to? | ___ | ___ | ___ |
| 10) Is there a contact or procedure in place to handle a power interruption in your office area? | ___ | ___ | ___ |
| 11) Are the computer and peripheral devices located away from any potential source of strong magnetic or electrical fields? | ___ | ___ | ___ |
| 12) Does the floor space layout and equipment arrangement promote maximum operational effectiveness? | ___ | ___ | ___ |
| 13) Are discarded computer listings and printouts thrown in office waste baskets? | ___ | ___ | ___ |
| Are printouts collected and stored for disposal? | ___ | ___ | ___ |

| | YES | NO | N/A |
|---|---|---|---|
| 14) If an extension cord is being used to connect the computer to a power outlet, does it carry the proper rating to handle the current required? | ___ | ___ | ___ |
| 15) Are peripherals also safely connected to a power outlet? | ___ | ___ | ___ |
| 16) Have precautions been taken to eliminate static electrical charges built up in personnel prior to their touching the computer? | ___ | ___ | ___ |
| 17) Is the computer located in an area where there is a noticeable buildup of dust or lint? | ___ | ___ | ___ |
| 18) Are periodic inspections made to ensure that there is no buildup of dust and lint over fan and ventilation areas of computer and peripherals? | ___ | ___ | ___ |

| **COMMUNICATIONS** | **YES** | **NO** | **N/A** |
|---|---|---|---|
| 1) If a modem is used with the computer, is it securely fastened to the computer and the table or work space? | ___ | ___ | ___ |
| 2) If the computer is attached to a local network, are connecting cables visible over their entire run? | ___ | ___ | ___ |
| 3) Is the computer set up to enable access from a remote location? | ___ | ___ | ___ |
| 4) If the computer is accessible from a remote location, is there a callback scheme to minimize the risk of access from an unauthorized person? | ___ | ___ | ___ |
| 5) If the computer is used to transmit and receive data, does the nature of the data require encryption procedures and equipment? | ___ | ___ | ___ |
| 6) If a modem is being used that requires a telephone be attached to establish communications, is it a general office extension or a dedicated line? | ___ | ___ | ___ |

| **USER AWARENESS & TRAINING** | **YES** | **NO** | **N/A** |
|---|---|---|---|
| 1) Is there a computer security and awareness training program for personnel at your facility? | ___ | ___ | ___ |
| 2) Are all persons who use the computer aware of their responsibilities for security? | ___ | ___ | ___ |
| 3) Are users instructed in the designation and importance of password protection? | ___ | ___ | ___ |
| 4) Are there provisions for training users in the use of the software running on the computer? | ___ | ___ | ___ |
| 5) Is the work of inexperienced users supervised and periodically checked? | ___ | ___ | ___ |
| 6) Are system users notified of system updates and changes as they occur? | ___ | ___ | ___ |

| **MAGNETIC STORAGE MEDIA** | **YES** | **NO** | **N/A** |
|---|---|---|---|
| 1) If floppy disks or magnetic tape storage are used, are provisions available to secure this media? | ___ | ___ | ___ |
| 2) Are floppy disks routinely left in the computer drive? | ___ | ___ | ___ |
| 3) Are backup copies of important programs and files maintained? | ___ | ___ | ___ |
| If so, are any stored at an off-site location? | ___ | ___ | ___ |
| 4) Do tapes and floppy disks have legible external labels indicating their contents? | ___ | ___ | ___ |
| 4) If users maintain their own floppy disk libraries, are they stored in a container to prevent damage and theft? | ___ | ___ | ___ |
| 6) Are there procedures for the moving of fixed head storage devices to prevent damage to the device? | ___ | ___ | ___ |
| 7) Are separate labels placed on floppy disks to indicate contents as opposed to writing directly on the disk cover? | ___ | ___ | ___ |

| **DATA & SYSTEM INTEGRITY** | **YES** | **NO** | **N/A** |
|---|---|---|---|
| 1) Is shared software protected from undetected modification? | ___ | ___ | ___ |
| 2) Are software licensing agreements and copyright restrictions adhered to? | ___ | ___ | ___ |
| 3) Are critical data files backed-up on a regular basis? | ___ | ___ | ___ |
| If so, are there several generations in the back-ups? | ___ | ___ | ___ |
| 4) Are copies of the system software running on the computer maintained? | ___ | ___ | ___ |
| 5) Are there provisions for recording changes to applications software and system software running on the computer? | ___ | ___ | ___ |
| 6) When a user no longer needs to use the computer, are there procedures in place to terminate their access to the system? | ___ | ___ | ___ |
| If so, is this process timely? | ___ | ___ | ___ |

| **DATA & SYSTEM ACCESS CONTROLS** | **YES** | **NO** | **N/A** |
|---|---|---|---|
| 1) If the computer system is intended for use only by specific users, are there adequate safeguards (physical or otherwise) to prevent unauthorized use? | ___ | ___ | ___ |
| 2) Does the computer operating system provide for levels of file protection for users? | ___ | ___ | ___ |
| 3) If the computer operating system requires logon id and password entry, are they displayed on the screen exactly as they are entered? | ___ | ___ | ___ |
| 4) Is the computer left "logged on" during the work day? | ___ | ___ | ___ |
| 5) Are users required to logoff the computer when they are called away for a length of time? | ___ | ___ | ___ |
| 6) Does system software provide for disabling terminal after a fixed number of signon attempts have occurred? | ___ | ___ | ___ |
| 7) If the system makes use of a database, are there controls to limit user access to and modifications of the contents of the database? | ___ | ___ | ___ |
| 8) Does the capability exist on the system to limit user access by means of specific menu formats based on user profiles? | ___ | ___ | ___ |

A discussion of the security subject areas covered by the checklist will serve to point out potential security strengths and weaknesses as they would apply to a microcomputer system undergoing evaluation. There is no correct answer to any of the questions as different installations and offices have different needs and configurations of equipment. While this checklist assessment is not a complete and all encompassing tool, it does touch on some of the major areas of security vulnerability related to microcomputers and will hopefully provide the user with an increased awareness of potential trouble areas that may need to be addressed.

Throughout the discussion that follows, suggestions are made and reasons given for implementing procedures and features outlined in the body of the checklist. As with any suggestion, the office performing this evaluation has to decide what procedures and features best suit the needs of the staff, mission, and budget in providing the most effective security environment practical.

**ADMINISTRATIVE:**

1) If your office owns the computer, then you have a vested interest in ensuring that all necessary security is provided for the computer. Owning the system that you work on will enable you to implement specific security requirements germane to your office functions and mission objectives. Being a user on a system that is controlled by an entity outside of your office places your security requirements in the hands of someone who may not share your concerns or needs relative to the type and level of security required to perform your job.

2) Of all the security measures available, this provides more security for the investment (free) than any of the expensive gadgets that can be bought. Users of the computer should be required to change their passwords on a periodic basis. By doing this, you will lessen the chance of a password becoming known and used by persons other than the assigned user. In assigning a password, instruct the users to avoid using a password that would involve something about their person or something associated with them (i.e. their name, car type, birth date, astrology sign, etc.). Consult the Administrative Security chapter of the AIS Security Manual (COMDTINST M5500.13), FIPS PUB 112, Password Usage, or the Department of Defense Password Management Guideline (CSC-STD-002-85) for further guidance in determining a password procedure.

3) The classification, if appropriate, of the data being processed on the computer is vital to determining what measures need to be taken to ensure a secure operating

environment. Ensuring that system users know what data is classified and what procedures are to be followed will go a long way in avoiding compromising of the data and the system. Likewise critical and sensitive data must be handled in accordance with the guidance that is provided in the Coast Guard Automated Information System (AIS) Security Manual.

4) A system administrator provides users with a point of reference for inquiries into system operations as well as ensure that the system is organized and operated under the guidance and supervision of a responsible, trained person. The system administrator handles the assignment of passwords, user access levels, file allocation and data backups just to name a few of the responsibilities. Consistency of operation and organization are the main benefits derived from making this appointment.

5) An ADP System Security Officer (ADPSSO), as the name implies, is a person who is responsible for ensuring the security of the computer system and compliance with the security guidelines and policy as set forth in the Coast Guard AIS Security Manual. Appointment of a person to fill this position will provide a point of contact through which security information and guidance may be obtained.

6) All valid users of the computer system need to be recognized as such by the operating system by means of a logon code and password, and by the system administrator who is responsible for keeping track of who is authorized to use the system. Allowing anyone access to the computer is inviting trouble and the possibility of the system and data integrity being compromised.

7) The development of a numbering scheme for floppy disks will provide a means of tracking the number in circulation and who has them within your office. Records of floppy disks should be kept to prevent theft, possible misuse of the storage media for personal gain and insuring that backup files are maintained and available if needed on readily referenced volumes.

8) When someone discovers that a piece of equipment or other item is missing, a report should be made to the responsible authority so that immediate steps may be taken to recover the resource. Confusion and delay in reporting a theft may make a difference in the speedy recovery or total loss of a resource.

**DOCUMENTATION:**

1) Current (and up to date) operating manuals provide users with a ready reference source to answer their questions should they need assistance in the absence of trained personnel. A confused and misinformed user could do significant damage to data and applications on your system.

2) If users who are unfamiliar with the computer system are allowed access, it is important for them to be made aware of specific operations and procedures that have been set up for the system. A guidebook or listing of these procedures will serve to alleviate confusion and frustration on the part of the user and the potential for inadvertent misuse of the system.

3) If the computer is used by more than one person in the office, maintain a usage log in the event that a situation arises where it would be important to know who was active on what terminal for a given time period.

4) Maintain a record of changes that have been made to system and application programs. To simply have someone make a change and fail to make a notation of the fact could lead to complicated and confusing auditing should a problem arise that requires knowledge of exactly what exists and how the system was designed to fuction. Anyone involved with altering of software should be aware of the correct change notation procedures for the office.

5) An up to date inventory of the data files, applications software, and system software for the computer will provide for a quicker recovery from a loss or disaster than if there were none at all. It is far easier to restore a system if you know exactly what was on it rather than to have to recover from bits and pieces of people's memories as to what was on it. Often, the creation and maintenance of backup files will further any recovery efforts.

6) Maintain a list of all the hardware components comprising the computer system in your office. Model numbers, serial numbers, memory sizes and other information about the hardware will facilitate recovery from a theft as well as a number of other threats where equipment has been damaged and must be repaired or replaced.

**PHYSICAL:**

1) Make sure that the location of the computer in the office is not in a heavily traveled thoroughfare in plain view of all, unless the computer's use requires that it be

freely accessible. More often than not, a passerby has the opportunity to do damage that may go undetected for quite some time.

2) Locking the door(s) that access the office area where the computer is located during off-hours will deter or prevent unauthorized use, theft or damage to the computer system.

3) If the janitorial staff has access to the office area where the computer is located, make sure that the names and the comings and goings of these persons are recorded in the event that they are needed. Also facilities and contractor personnel should have their names and whereabouts recorded.

4) Most desktop computers are compact and light enough that they can be easily removed and taken away from the office by virtually anyone. A lockdown device or bolting the computer cabinet to the work space provides an additional deterrent to a would be thief and makes their task more difficult if not impossible.

5) If a person can't turn the computer on, they can't use it! Keyed power switches or lockable access covers to the power switch are positive means of preventing misuse of computer resources by unauthorized persons.

6) If the keyboard for the computer is not an integral part of the base cabinet housing, it can become a prime target for removal and theft by simply disconnecting it from the terminal. Secure an attached keyboard, as you would the terminal housing, to the work space. Also, insure that the connecting cable is securely fastened so that contact is maintained between the keyboard and the terminal.

7) A computer terminal screen that can be easily viewed by parties not involved with the system use can compromise a system as quickly as a deliberate access by an unauthorized user. Need to know and see apply when an application is being run on the computer where the data being processed is visible on the screen.

8) As with the terminal and keyboard, a table top printer can be removed with little difficulty. Take steps to secure the printer to a work table as you should all compact system devices.

9) The printer should be located away from main access paths through the office area. It is unnecessary for anyone other than the concerned parties to view printouts that are being produced on the machine. The vulnerability to disclosure or theft of information from a casual passerby can be lessened by locating the printer in a more

| **ENVIRONMENTAL** | **YES** | **NO** | **N/A** |
|---|---|---|---|
| 1) Is the computer located where it is directly exposed to sunlight? | | | |
| Extreme heat? | ___ | ___ | ___ |
| Extreme Cold? | ___ | ___ | ___ |
| 2) Is there an approved class fire extinguisher readily accessible in the area where the computer is located? | ___ | ___ | ___ |
| 3) Is there adequate ventilation around the computer and any peripheral devices to prevent heat buildup? | ___ | ___ | ___ |
| 4) Are there smoke/fire detectors in the immediate area of the computer? | ___ | ___ | ___ |
| 5) Are computer cables and power cords arranged and maintained so as not to pose a fire hazard or safety hazard to personnel? | ___ | ___ | ___ |
| 6) Is the area where the computer is located equipped with raised flooring? | ___ | ___ | ___ |
| 7) Does the electrical circuit the computer is plugged into carry a sufficient current for the equipment to operate on? | ___ | ___ | ___ |
| 8) Is there a voltage surge suppressor or regulator installed to protect the computer and peripheral devices from power spikes or surges? | ___ | ___ | ___ |
| 9) Are there frequent, observable power interruptions on the circuit that the computer is connected to? | ___ | ___ | ___ |
| 10) Is there a contact or procedure in place to handle a power interruption in your office area? | ___ | ___ | ___ |
| 11) Are the computer and peripheral devices located away from any potential source of strong magnetic or electrical fields? | ___ | ___ | ___ |
| 12) Does the floor space layout and equipment arrangement promote maximum operational effectiveness? | ___ | ___ | ___ |
| 13) Are discarded computer listings and printouts thrown in office waste baskets? | ___ | ___ | ___ |
| Are printouts collected and stored for disposal? | ___ | ___ | ___ |

| | YES | NO | N/A |
|---|---|---|---|
| 14) If an extension cord is being used to connect the computer to a power outlet, does it carry the proper rating to handle the current required? | ___ | ___ | ___ |
| 15) Are peripherals also safely connected to a power outlet? | ___ | ___ | ___ |
| 16) Have precautions been taken to eliminate static electrical charges built up in personnel prior to their touching the computer? | ___ | ___ | ___ |
| 17) Is the computer located in an area where there is a noticeable buildup of dust or lint? | ___ | ___ | ___ |
| 18) Are periodic inspections made to ensure that there is no buildup of dust and lint over fan and ventilation areas of computer and peripherals? | ___ | ___ | ___ |

sources of heat only serves to further strain and stress the tolerance of the components. Extreme cold is not so much a threat to the hardware components as to the storage media and the human users of the system. An office environment that is tolerable for humans is probably tolerable for the computer.

2) Having an approved class fire extinguisher readily accessible within the proximity of the computer is a must. The fire extinguisher should have an electrical fire classification and be kept in proper working order and fully charged. All personnel should be made familiar with the extinguishers location, operation, and inspection procedures.

3) Install the computer so that there is an adequate circulation of air all about the component housings. This will aid in dissipating heat buildup and help to keep particulate matter from settling into the component casings and openings. Heat and dust buildup will shorten the life of the computer and may precipitate costly repairs.

4) A "NO" answer to this question should create some serious concern. The foremost concern should be for the safety and well being of the personnel in the office. Some form of smoke or fire detection device should be prevalent in the office area. The computer can be replaced, the employee may not be such an easy loss to recover from.

5) By ensuring that computer power cords and connecting cables are safely and securely arranged, disruptions to service will be avoided by someone inadvertently tripping over a cord or cable and disconnecting or damaging both the equipment and the employee. Prevent overloading of outlets and circuits providing power to the computer system components as well as other office equipment.

6) If raised flooring is available in the area where the computer is located, cables and connections may be made underneath and out of sight of personnel. While this will serve to eliminate tripping and possible cable damage, periodic checks will need to be made to ensure that the cables have not been tampered with or damaged due to unobservable factors in the day to day operations.

7) Make sure that the electrical circuit supplying the computer and other system components is of a sufficient amperage to handle the load of all the system equipment. Outages due to overloading a circuit can cause delays in system usage as well as damage to equipment and building circuitry.

8) On the other end of the spectrum, if necessary precautions are not taken to guard against voltage spikes or power surges, serious damage can result to the delicate internal components of the computer system. The costly repairs and system downtime make these devices a good investment for the money.

9) A steady reliable source of uninterrupted power is a must for operating a computer system. System outages due to power fluctuations and loss is unacceptable when addressing data and system integrity. If the computer facility experiences frequent power outages or voltage drops, an uninterruptable power source might be an advisable countermeasure.

10) If the office area experiences a power outage, ensure that individuals know where to call or who to contact to restore service. Many times the power outage is of a local nature and will be unnoticed by a majority of the building.

11) Strong magnetic and electrical fields have a nasty habit of erasing and scrambling the careful arrangement of the data patterns that the computer has been instructed to establish on the storage media. Strong electrical currents will also impede or alter transmissions over communications lines and cables. Inspect the computer installation to ensure that the cabinetry and cabling is located away from high voltage lines and sources of magnetism.

12) Arrange the components of the computer system so that there is a logical and practical flow between devices. Don't locate a terminal several hundred feet from it's dedicated storage unit or printer. If a person has to get up from the terminal and travel to another office to receive their printout, someone may come along and make use of the access afforded a logged on terminal device unbeknownst to the acknowledged user.

13) An incredible amount of information can be gleaned from the trash created by a computer system. Discarded computer listings and outdated manuals are ready sources of information about an organization and the business conducted within. Arrange to accumulate discarded listings and system information for proper disposal to prevent an inadvertent disclosure.

14) If an extension cord must be used, ensure that the cord bears the Underwriters Laboratories approval and is constructed to handle the amperage required by the computer. An extension cord with a fusable connection will provide some protection against power surges and spikes.

15) Likewise, computer peripheral devices need the same care and attention to their power needs as does the computer itself. What good would the computer be if, say, the hard disk storage device kept shorting out?

16) This may seem like a trivial matter but, the effects of a static electrical charge on a floppy disk touched by a person can be as devastating as having the floppy disk stolen. A person carrying a strong static charge and then touching a keyboard can short out delicate circuitry within the computer itself. Antistatic floor coverings and treatments to remove static charge from the surroundings will help minimize this threat.

17) If lint and dust buildup are a problem, move the computer to a new location or take steps to eliminate the sources of the dust and lint. A sound deadening/dust containing printer cover is a means of addressing the paper dust that a printer produces as well as the sound.

18) A periodic check of ventilation ports and fan openings should be made to the computer system components so equipped. Denial of good ventilation leads to heat buildup and heat buildup leads to component failure and system downtime.

**COMMUNICATIONS:**

1) Most communications modems in use with a desk top computer are compact and transportable. As with the other system devices, the modem also needs to have steps taken to ensure that it will not "walk away." Secure connectors and fastening the modem to the work station will help prevent it's disappearing.

2) The ability to visually observe the run of a communication cable within a computer network will allow the user to check to see if the line has been tapped into or otherwise altered to permit interception of the signals being carried over the cable. Sometimes the lines are encased in a metal conduit to insure security but in many instances, communications, as well as other cables, are strung above a suspended ceiling where they are out of sight and out of mind.

3) The concept of distributed or remote access and processing has its advantages as well as disadvantages. A computer that can be accessed via telephone communications is open to anyone who can determine or acquire the number and operation codes and commands. Advisable security countermeasures would be frequent changing of system access passwords and commands as well

as an authorized user callback scheme. This problem is more of a concern to the mini/mainframe computer environment than that which this questionnaire will address. Still, if it applies it should be evaluated.

4) The use of a callback scheme operates as follows;

- a system user establishes contact with the computer at the office from a remote site over a telephone line.

- the computer then disconnects and dials the site telephone number that has been stored in a table of authorized users for the particular user in question.

- communications are then established to allow normal processing between the authorized user and the host computer.

As was mentioned above, this type of elaborate system verification scheme more readily translates to the power of a mini/mainframe environment than to a desk top computer.

5) Based on the nature and sensitivity of the data being processed by the computer, encryption may be a requirement for data transmission. Refer to the AIS Security Manual regarding classification of data and appropriate handling.

6) If a modem is connected to the computer, provide a dedicated extension or telephone line to use rather than a general usage office extension or line. A communications link might be established only to be broken because someone in the office mistakenly or purposely picked up on the line being used by the computer.

**USER AWARENESS & TRAINING:**

1-6) Of all the items and countermeasures that are available to provide computer security, training will get you the most return for the investment made. By far, the threat that has the greatest frequency of occurence and the most preventable is the threat of the uneducated user and the damage they can do. An office computer security awareness program will go a long way towards ensuring an office computer environment that is protected from a multitude of threats befalling many computer installations. An educated user is a smarter and more efficient user of the system resources. Ensure that persons using the computer system are educated as to the usage of the hardware as well as the system and application software that resides on the equipment. Instruct users in the correct usage and care of their system access codes and passwords and make them aware of system updates and changes as they are implemented. Of prime importance is to instill in the users the concept

that the information they will be processing is a valuable asset of the organization and as such, should be treated with the same care as the computer itself.

**CONTINGENCY PLANNING:**

1-6) Contingency planning is often thought of as pertaining only to a very large computer facility, such as a mainframe or minicomputer operation. While this is generally true, the desk top microcomputer may serve just as important a function as the mainframe or minicomputer in the organization. If the answer to question 6 was "YES", then the topic of contingency planning has a direct bearing on the organization. The purpose of the contingency plan is to minimize any delays or disruptions in service to users of the targeted computer resources. If the microcomputer were to become inoperative or unavailable for some reason, could the office perform the functions required to get the job done? More often than not, the answer is "NO." Therefore, some provisions should be made to address a contingency plan for the microcomputer. Some of the areas that should be considered for a microcomputer contingency plan might be;

- Availability of or access to backup hardware

- Storage of backup data files, application programs, and system software

- Maintenance and repair agreements with vendors

- Points of contact for physical plant resources (i.e. electricity, air conditioning)

- Hardware and software inventory controls

- Designation of system security officer

- Designation of a remote or alternate processing site

and many other areas that are germane to the functions performed by the office.

Members of the contingency planning team(s) within the organization should know the contents of the contingency plan and what their responsibilities are in the event the plan should have to be inacted. Preparing a contingency plan is important, but so is the testing of the plan to make sure that the actions specified in the plan are reasonable and executable. Periodic review and testing of the contingency plan will insure that the plan addresses the current computer processing needs of the organization that it was designed for. Better to have planned for an emergency situation and the needed action to be taken when it arises, than to throw one's hands in the air while making excuses for delayed or lost work because no one took the time to prepare a contingency plan.

**MAINTENANCE:**

1) A maintenance contract is an important feature to have in place to ensure that the system hardware components and software will function as planned for. The specific terms and the duration of the contract should be carefully examined and someone should be appointed to ensure that the terms and conditions of the contract are adhered to.

2) Preventative maintenance will go a long way in extending the life of the hardware on the system. Routine cleaning and adjustments will ensure that components function as specified by the manufacturer and in most cases, this is required to maintain the warranty on the equipment.

3) The designation of a point of contact within your organization, for equipment repairs and vendor inquiries, will help to eliminate any confusion between the users and the provider of the required services.

4) If the maintenance agreement provides for on-site service, make sure that the response time is acceptable to the organization. If the computer can remain idle for no more than three hours, a 48 hour response time agreement will do little good to restoring operations within the necessary time frame.

5) A user trouble log should be kept noting all instances of downtime and the reasons if known. Maintaining a log of this nature may prove invaluable in isolating a trouble area with the system and taking steps to rectify the situation.

6) This goes back to the awareness and training area. If the users know how to care for and correctly operate the system resources, they can expect to derive maximum use and efficiency from the system resources.

**MAGNETIC STORAGE MEDIA:**

1) Storage of data and programming files on floppy disk and/or magnetic tape should include providing for the security and safety of this media. Archive and backup files should be protected against exposure to accidental erasure or alteration as well as physical damage and the media being misplaced. A system administrator would be a good person to assign the duties of maintaining an orderly and secure storage program for these storage media.

2) Leaving a floppy disk in a computer drive long after it has served it's purpose is inviting trouble. The

potential for theft, accidental erasure or writeover is very real.

3) The need for backup files of important data and program files is important for contingency planning as was discussed earlier. The most important files should be candidates for backup and off-site storage to eliminate the possibility of their being lost to the organization should a disaster destroy the on-site resources.

4) A procedure for labeling of tapes and floppy disks should be implemented by the office or organization. Clearly labeling tapes and floppy disks as to their contents will help eliminate wasted time and confusion in searching for a file when no labels or poorly prepared labels are used. This will also help prevent any accidental erasure or writeover of files from not knowing what was on the tapes or disks.

5) Encourage users to store their floppy disks in containers that will protect them from physical abuse and theft. Often, simply placing them back in the box that they are purchased in is a good step to safeguarding the disks.

6) This is a precautionary measure that will probably not arise that often. Still, procedures should be in place should an office require that a fixed disk device be moved or relocated. These devices are not as forgiving as the floppy disk drives in most terminals and should have the manufacturer's instructions adhered to for the safety and operation of the equipment.

7) In addressing the labeling of floppy disks, **never** write directly on the disk jacket or protective cover. Use the labels that are provided with the disks and prepare them prior to placing them on the disks. The physical pressure of writing on the jacket may be enough to distort the disk and damage the drive when a read or write function is invoked.

**DATA & SYSTEM INTEGRITY:**

1) Measures should be taken to ensure that users of shared software are not able to alter the software in any way, shape, or form. This is most easily accomplished by setting protection levels to permit read and execute access only.

2) Software licensing agreements and copyright restrictions are legally binding requirements for the use of virtually all purchased software products. Make sure that the provisions of such agreements are fully disclosed and understood by users of these products. Ignorance is a poor excuse in a liability suit.

3) Critical data files should be backed up periodically based on program needs and requirements. In some cases, more than one backup copy is called for and possibly several generations will be required to recreate lost or damaged files. The idea of maintaining several generations comes into play if a problem is discovered that has persisted for a period of time rendering, say, the last two backup files useless.

4) Current, up to date copies of system software should be maintained as well as data and application files. The organization's data and applications would be of little use if the computer operating system software were lost along with the hardware.

5) All changes to any software operating on the computer must be recorded. In addition to recording the changes, users should be notified if these changes will effect the way they do business on the computer. Software surprises are seldom appreciated.

6) When an employee no longer requires access to the services of the computer system, make sure that their access code and password are removed from the system. This should be done as quickly as possible after notification. Leaving an unauthorized user access to the system is like leaving a car open with the keys in the ignition, an invitation to trouble.

**DATA & SYSTEM ACCESS CONTROLS:**

1) Most of the areas addressed by this checklist are aimed at providing a secure operating environment for the users of a computer system. A computer system will generally be established for a specific group of users and measures should be provided to guarantee the integrity and availability of the system for those users.

2) Setting file protection levels is an important feature for the operating system software to afford the users. This feature will enable users to selectively assign access to programs and files according to program and personnel needs.

3) Most computer operating systems have provisions for a logon sequence to identify authorized users of the system. The user enters a logon code which is usually followed by a unique user password identifier. Provisions to guard against the inadvertent disclosure of either of these elements of system access should be implemented. Some system software displays disguise characters in place of the actual sequence of characters

keystroked (i.e. the Standard Terminal software displaying "#" symbols instead of the actual keyboard symbols pressed when entering a password).

4-5) The practice of logging onto a system at the start of a business day and remaining logged on throughout the day is inviting disaster. Unless the office is physically secure and there is no change that an outsider or passerby could use the terminal(s), users should log onto a system when they require access and log off the system when their work is complete or if they will be away from the terminal for an extended period of time.

6) A system software feature that allows for a predetermined number of signon attempts before the system locks out the terminal or the logon identifier being used is a useful security precaution. This usually requires that the system administrator go into the operating system to "unlock" the user identifier or terminal before it may be used again. Some may complain that this type of protection penalizes an authorized user of the system who simply forgot their logon identifier as well as the unauthorized intruder. The inconvenience will probably be insignificant when compared to the damage an unauthorized user could wreak on the system.

7) A database is an important repository of information forming the basis of many computer applications. The importance of this resource dictates that steps be taken to address the safety and security of the information stored in it. The system administrator or database administrator should provide for required access features as well as who and what will be allowed to be modified or deleted. Unauthorized access to a database coupled with unrestricted modification can bring an organization to a standstill in the event that data is lost or destroyed inadvertently or on purpose.

8) Menus tailored to user needs are a viable means of controlling system access. If a user only needs to access one particular file to execute a system application, a user profile could be established that will permit them to get at only those files required to execute the application. The phrase "need to know" might be changed to "need to use" in these cases.

In summation, "NO" answers to questions on the checklist are areas that are candidates for evaluation and possible corrective action. While some of the questions may not be applicable to the environment at present, they should be kept in mind when future changes are being considered by the organization.

December 12, 1985

CIRCULAR NO. A-130

TO THE HEADS OF EXECUTIVE DEPARTMENTS AND ESTABLISHMENTS

SUBJECT: Management of Federal Information Resources

1. Purpose: This Circular establishes policy for the management of Federal information resources. Procedural and analytic guidelines for implementing specific aspects of these policies are included as appendices.

2. Rescissions: This Circular rescinds OMB Circulars No. A-71, A-90, A-108, and A-121, and all Transmittal Memoranda to those circulars.

3. Authorities: This Circular is issued pursuant to the Paperwork Reduction Act of 1980 (44 U.S.C. 35); the Privacy Act of 1974 (5 U.S.C. 552a), Sections 111 and 206 of the Federal Property and Administrative Services Act of 1949 as amended (40 U.S.C. 759 and 487, respectively), the Budget and Accounting Act of 1921 as amended (31 U.S.C. 11), Executive Order No. 12046 of March 27, 1978, and Executive Order No. 12472 of April 3, 1984.

4. Applicability and Scope:

   a. The policies in this Circular apply to the information activities of all agencies of the executive branch of the Federal Government.

   b. Information classified for national security purposes should also be handled in accordance with the appropriate national security directives. National security emergency preparedness activities should be conducted in accordance with Executive Order No. 12472.

5. Background: The Paperwork Reduction Act establishes a broad mandate for agencies to perform their information management activities in an efficient, effective, and economical manner. To assist agencies in an integrated approach to information resources management, the Act requires that the Director of the Office of Management and Budget (OMB) develop and implement uniform and consistent information resources management policies; oversee the development and promote the use of information management principles, standards, and guidelines; evaluate agency information management practices in order to determine their adequacy and efficiency; and determine compliance of such practices with the policies, principles, standards, and guidelines promulgated by the Director.

6. Definitions: As used in this Circular--

a. The term "agency" means any executive department, military department, government corporation, government controlled corporation, or other establishment in the executive branch of the government, or any independent regulatory agency. Within the Executive Office of the President, the term includes only the Office of Management and Budget and the Office of Administration.

b. The term "information" means any communication or reception of knowledge such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any medium, including computerized data bases, paper, microform, or magnetic tape.

c. The term "government information" means information created, collected, processed, transmitted, disseminated, used, stored, or disposed of by the Federal Government.

d. The term "information system" means the organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual.

e. The term "major information system" means an information system that requires special continuing management attention because of its importance to an agency mission; its high development, operating or maintenance costs; or its significant impact on the administration of agency programs, finances, property, or other resources.

f. The term "access to information" refers to the function of providing to members of the public, upon their request, the government information to which they are entitled under law.

g. The term "dissemination of information" refers to the function of distributing government information to the public, whether through printed documents, or electronic or other media. "Dissemination of information" does not include intra-agency use of information, interagency sharing of information, or responding to requests for "access to information."

h. The term "information technology" means the hardware and software used in connection with government information, regardless of the technology involved, whether computers, telecommunications, micrographics, or others. For the purposes of this Circular, automatic data processing and telecommunications activities related to certain critical national security missions, as defined in 44 U.S.C. 3502 (2) and 10 U.S.C. 2315, are excluded.

i. The term "information technology facility" means an organizationally defined set of personnel, hardware, software, and physical facilities, a primary function of which is the operation of information technology.

j. The term "information resources management" means the planning, budgeting, organizing, directing, training, and control associated with government information. The term encompasses both information itself and the related resources, such as personnel, equipment, funds, and technology.

k. The term "government publication" means informational matter which is published as an individual document at government expense, or as required by law.

Other definitions specific to the subjects of the appendices appear in the appendices.

7. Basic Considerations and Assumptions

a. The Federal Government is the largest single producer, consumer, and disseminator of information in the United States. Because of the size of the government's information activities, the dependence of government information activities upon the public's cooperation, and the value of government information to the entire Nation, the management of Federal information resources is an issue of continuing importance to the public and to the government itself.

b. Government information is a valuable national resource. It provides citizens with knowledge of their government, society, and economy--past, present, and future; is a means to ensure the accountability of government; is vital to the healthy performance of the economy; is an essential tool for managing the government's operations; and is itself a commodity often with economic value in the marketplace.

c. The free flow of information from the government to its citizens and vice versa is essential to a democratic society. It is also essential that the government minimize the Federal paperwork burden on the public, minimize the cost of its information activities, and maximize the usefulness of government information.

d. In order to minimize the cost and maximize the usefulness of government information activities, the expected public and private benefits derived from government information, insofar as they are calculable, should exceed the public and private costs of the information.

e. Although certain functions are inherently governmental in nature, being so intimately related to the public interest as to mandate performance by Federal employees, the government

should look first to private sources where available, to provide the commercial goods and services needed by the government to act on the public's behalf, particularly when cost comparisons indicate that private performance will be the most economical.

f. The use of up-to-date information technology offers opportunities to improve the management of government programs, and access to, and dissemination of, government information.

g. Because the public disclosure of government information is essential to the operation of a democracy, the public's right of access to government information must be protected in the management of Federal information resources.

h. The individual's right to privacy must be protected in Federal Government information activities involving personal information.

i. The open and efficient exchange of government scientific and technical information, subject to applicable national security controls and proprietary rights others may have in-such information, fosters excellence in scientific research and the effective use of Federal research and development funds.

j. The value of preserving government records is a function of the degree to which preservation protects the legal and financial rights of the government or its citizens, and provides an official record of Federal agency activities for agency management, public accountability, and historical purposes.

k. Federal Government information resources management policies and activities can affect, and be affected by, the information policies and activities of other nations.

8. Policies

a. Information Management. Agencies shall:

(1) Create or collect only that information necessary for the proper performance of agency functions and that has practical utility, and only after planning for its processing, transmission, dissemination, use, storage, and disposition;

(2) Seek to satisfy new information needs through legally authorized interagency or intergovernmental sharing of information, or through commercial sources, where appropriate, before creating or collecting new information;

(3) Limit the collection of individually identifiable information and proprietary information to that which is legally authorized and necessary for the proper performance of agency functions;

(4) Maintain and protect individually identifiable information and proprietary information in a manner that precludes:

(a) Unwarranted intrusion upon personal privacy (see Appendix I); and

(b) Violation of confidentiality;

(5) Provide individuals with access to, and the ability to amend errors in, systems of records, consistent with the Privacy Act;

(6) Provide public access to government information, consistent with the Freedom of Information Act;

(7) Ensure that agency personnel are trained to safeguard information resources;

(8) Disseminate information, as required by law, describing agency organization, activities, programs, meetings, systems of records, and other information holdings, and how the public may gain access to agency information resources;

(9) Disseminate such information products and services as are:

(a) Specifically required by law; or

(b) Necessary for the proper performance of agency functions, provided that the latter do not duplicate similar products or services that are or would otherwise be provided by other government or private sector organizations;

(10) Disseminate significant new, or terminate significant existing, information products and services only after providing adequate notice to the public;

(11) Disseminate such government information products and services:

(a) In a manner that ensures that members of the public whom the agency has an obligation to reach have a reasonable ability to acquire the information;

(b) In the manner most cost effective for the government, including placing maximum feasible reliance on the private sector for the dissemination of the products or services in accordance with OMB Circular No. A-76; and

(c) So as to recover costs of disseminating the products or services through user charges, where appropriate, in accordance with OMB Circular No. A-25;

(12) Establish procedures for:

(a) Reviewing periodically the continued need for and manner of dissemination of the agency's information products or services; and

(b) Ensuring that government publications are made available to depository libraries as required by law.

b. Information Systems and Information Technology Management. Agencies shall:

(1) Establish multiyear strategic planning processes for acquiring and operating information technology that meet program and mission needs, reflect budget constraints, and form the bases for their budget requests;

(2) Establish systems of management control that document the requirements that each major information system is intended to serve; and provide for periodic review of those requirements over the life of the system in order to determine whether the requirements continue to exist and the system continues to meet the purposes for which it was developed;

(3) Make the official whose program an information system supports responsible and accountable for the products of that system;

(4) Meet information processing needs through interagency sharing and from commercial sources, when it is cost effective, before acquiring new information processing capacity;

(5) Share available information processing capacity with other agencies to the extent practicable and legally permissible;

(6) Acquire information technology in a competitive manner that minimizes total life cycle costs;

(7) Ensure that existing and planned major information systems do not unnecessarily duplicate information systems available from other agencies or from the private sector;

(8) Acquire off-the-shelf software from commercial sources, unless the cost effectiveness of developing custom software is clear and has been documented;

(9) Acquire or develop information systems in a manner that facilitates necessary compatibility;

(10) Assure that information systems operate effectively and accurately;

(11) Establish a level of security for all agency information systems commensurate with the sensitivity of the information and the risk and magnitude of loss or harm that could result from improper operation of the information systems (See Appendix III);

(12) Assure that only authorized personnel have access to information systems;

(13) Plan to provide information systems with reasonable continuity of support should their normal operations be disrupted in an emergency;

(14) Use Federal Information Processing and Telecommunications Standards except where it can be demonstrated that the costs of using a standard exceed the benefits or the standard will impede the agency in accomplishing its mission;

(15) Not require program managers to use specific information technology facilities or services unless it is clear and is convincingly documented, subject to periodic review, that such use is the most cost effective method for meeting program requirements;

(16) Account for the full costs of operating information technology facilities and recover such costs from government users as provided in Appendix II;

(17) Not prescribe Federal information system requirements that unduly restrict the prerogatives of heads of State and local government units;

(18) Seek opportunities to improve the operation of government programs or to realize savings for the government and the public through the application of up-to-date information technology to government information activities.

9. Assignment of Responsibilities:

a. All Federal Agencies. The head of each agency shall:

(1) Have primary responsibility for managing agency information resources;

(2) Ensure that the information policies, principles, standards, guidelines, rules, and regulations prescribed by OMB are implemented appropriately within the agency;

(3) Develop internal agency information policies and procedures and oversee, evaluate, and otherwise periodically review agency information resources management activities for conformity with the policies set forth in this Circular;

(4) Develop agency policies and procedures that provide for timely acquisition of required information technology;

(5) Maintain an inventory of the agencies' major information systems and information dissemination programs;

(6) Create, maintain, and dispose of a record of agency activities in accordance with the Federal Records Act of 1950, as amended;

(7) Identify to the Director, OMB, statutory, regulatory, and other impediments to efficient management of Federal information resources and recommend to the Director legislation, policies, procedures, and other guidance to improve such management;

(8) Assist OMB in the performance of its functions under the Paperwork Reduction Act, including making services, personnel, and facilities available to OMB for this purpose to the extent practicable;

(9) Appoint a senior official, as required by 44 U.S.C. 3506(b), who shall report directly to the agency head, to carry out the responsibilities of the agency under the Paperwork Reduction Act. The head of the agency shall keep the Director, OMB, advised as to the name, title, authority, responsibilities, and organizational resources of the senior official. For purposes of this paragraph military departments and the Office of the Secretary of Defense may each appoint one official.

b. Department of State. The Secretary of State shall:

(1) Advise the Director, OMB, on the development of United States positions and policies on international information policy issues affecting Federal Government information activities and ensure that such positions and policies are consistent with Federal information resources managment policy;

(2) Ensure, in consultation with the Secretary of Commerce, that the United States is represented in the development of international information technology standards, and advise the Director, OMB, of such activities.

c. Department of Commerce. The Secretary of Commerce shall:

(1) Develop and issue Federal Information Processing Standards and guidelines necessary to ensure the efficient and effective acquisition, management, security, and use of information technology;

(2) Advise the Director, OMB, on the development of policies relating to the procurement and management of Federal telecommunications resources;

(3) Provide OMB and the agencies with scientific and technical advisory services relating to the development and use of information technology;

(4) Conduct studies and evaluations concerning telecommunications technology, and concerning the improvement, expansion, testing, operation, and use of Federal telecommunications systems and advise the Director, OMB, and appropriate agencies of the recommendations that result from such studies;

(5) Develop, in consultation with the Secretary of State and the Director, OMB, plans, policies, and programs relating to international telecommunications issues affecting government information activities;

(6) Identify needs for standardization of telecommunications and information processing technology, and develop standards, in consultation with the Secretary of Defense and the Administrator of General Services, to ensure efficient application of such technology;

(7) Ensure that the Federal Government is represented in the development of national and, in consultation with the Secretary of State, international information technology standards, and advise the Director, OMB, of such activities.

d. Department of Defense. The Secretary of Defense shall develop, in consultation with the Administrator of General Services, uniform Federal telecommunications standards and guidelines to ensure national security, emergency preparedness, and continuity of government.

e. General Services Administration. The Administrator of General Services shall:

(1) Advise the Director, OMB, and agency heads on matters affecting the procurement of information technology;

(2) Coordinate and, when required, provide for the purchase, lease, and maintenance of information technology required by Federal agencies;

(3) Develop criteria for timely procurement of information technology and delegate procurement authority to agencies that comply with the criteria;

(4) Provide guidelines and regulations for Federal agencies, as authorized by law, on the acquisition, maintenance, and disposition of information technology;

(5) Develop policies and guidelines that facilitate the sharing of information technology among agencies as required by this Circular;

(6) Review agencies' information resources management activities to meet the objectives of the triennial reviews required by the Paperwork Reduction Act and report the results to the Director, OMB;

(7) Manage the Automatic Data Processing Fund and the Federal Telecommunications Fund in accordance with the Federal Property and Administrative Services Act, as amended;

(8) Establish procedures for approval, implementation, and dissemination of Federal telecommunications standards and guidelines and for implementation of Federal Information Processing Standards.

f. Office of Personnel Management. The Director, Office of Personnel Management, shall:

(1) Develop and conduct training programs for Federal personnel on information resources management, including end user computing;

(2) Evaluate periodically future personnel management and staffing requirements for Federal information resources management;

(3) Establish personnel security policies and develop training programs for Federal personnel associated with the design, operation, or maintenance of information systems.

g. National Archives and Records Administration. The Archivist of the United States shall:

(1) Administer the Federal records management program in accordance with the National Archives and Records Act;

(2) Assist the Director, OMB, in developing standards and guidelines relating to the records management program.

h. Office of Management and Budget. The Director of the Office of Management and Budget shall:

(1) Provide overall leadership and coordination of Federal information resources management within the executive branch;

(2) Serve as the President's principal adviser on procurement and management of Federal telecommunications systems, and develop and establish policies for procurement and management of such systems;

(3) Issue policies, procedures, and guidelines to assist agencies in achieving integrated, effective, and efficient information resources management;

(4) Initiate and review proposals for changes in legislation, regulations, and agency procedures to improve Federal information resources management;

(5) Review and approve or disapprove agency proposals for collection of information from the public, as defined in 5 CFR 1320.7;

(6) Develop and publish annually, in consultation with the Administrator of General Services, a five-year plan for meeting the information technology needs of the Federal government;

(7) Evaluate agencies' information resources management and identify cross-cutting information policy issues through the review of agency information programs, information collection budgets, information technology acquisition plans, fiscal budgets, and by other means;

(8) Provide policy oversight for the Federal records management function conducted by the National Archives and Records Administration and coordinate records management policies and programs with other information activities;

(9) Review, with the advice and assistance of the Administrator of General Services, selected agencies' information resources management activities to meet the objectives of the triennial reviews required by the Paperwork Reduction Act;

(10) Review agencies' policies, practices, and programs pertaining to the security, protection, sharing, and disclosure of information, in order to ensure compliance with the Privacy Act and related statutes;

(11) Resolve information technology procurement disputes between agencies and the General Services Administration pursuant to Section 111 of the Federal Property and Administrative Services Act;

(12) Review proposed U.S. government position and policy statements on international issues affecting Federal Government information activities and advise the Secretary of State as to their consistency with Federal information resources management policy.

10. Oversight. The Director, OMB, will use information technology planning reviews, fiscal budget reviews, information collection budget reviews, management reviews, GSA reviews of agency information resources management activities, and such

other measures as he deems necessary to evaluate the adequacy and efficiency of each agency's information resources management and compliance with this Circular.

11. Effective Date. This Circular is effective upon publication.

12. Inquiries. All questions or inquiries should be addressed to Office of Information and Regulatory Affairs, Office of Management and Budget, Washington, D.C. 20503. Telephone: (202) 395-3287.

13. Sunset Review Date. This Circular shall have an independent policy review to ascertain its effectiveness three years from the date of issuance.

James III
Director

Appendix I: Federal Agency Responsibilities for Maintaining Records about Individuals

Appendix II: Cost Accounting, Cost Recovery, and Interagency Sharing of Information Technology Facilities

Appendix III: Security of Federal Automated Information Systems

Appendix IV: Analysis of Key Sections